이진 행렬을 적용한 DSM 설계 원리에 대한 고찰*

*김태현 **정기태 ***성재철 ****홍석희
고려대학교 정보경영공학전문대학원
*kimth714@cist.korea.ac.kr

On the Construction of Diffusion switching Mechanism using Binary Matrices

*Taehyun Kim **Kitae Jeong ***Jaechul Sung ****Seokhie Hong
Graduate School of Information Management and Security, Korea University

요 약

Shirai 등은 FSE'04에서 DSM 설계 원리를 적용하여 증명 가능한 Feistal 구조를 제안하였다. 제안된 구조는 임의의 라운드 수에 대하여 능동 S-box의 최소 개수를 증명할 수 있다. 그러나 제안된 구조에 제약된 조건을 만족하는 행렬이 존재함을 증명하지 못하였다. 본 논문에서는 DSM 설계 원리에 최대 branch number를 갖는 $m \times m$ 이진 행렬을 적용하였을 경우 동일한 최대 branch number를 가지지 못함을 증명한다 ($m \leq 34$). 이는 이진 행렬을 이용하여 Shirai 등이 제안한 구조를 설계할 수 없음을 의미한다.

1. 서론

블록 암호는 외부로부터 데이터를 보호하기 위한 방법으로 오랫동안 사용되어온 대칭키 암호 알고리즘이다. 블록 암호는 Shannon의 정보 이론 [7]에 근거하여 대치와 치환의 반복 과정으로 개발되었으며 DES가 미국연방표준으로 채택된 이후 블록 암호의 설계 원리와 안전성 분석에 대한 본격적인 연구가 시작되었다. 특히, 90년대 초에 차분 공격 [2]과 선형 공격 [4]이 소개된 이후, 블록 암호의 안전성 분석과 설계에 대한 이론을 구축하는데 큰 역할을 하였고 안전성이 증명 가능한 블록 암호의 구조에 대한 연구가 진행되었다. 그 결과, 차분 공격과 선형 공격에 안전한 S 박스와 좋은 확산 효과를 갖는 함수에 대한 이론들이 도출되었고 optimal diffusion 개념이 블록 암호의 설계에 적용되었다. Optimal diffusion은 최대 branch number를 갖는 선형 변환 함수로서 AES를 비롯한 최근의 블록 암호의 설계에 있어 널리 사용되고 있다.[1,3,5,6]

Shirai 등은 [9]에서 MDS 행렬을 이용하여 차분 공격과 선형 공격에 안전성이 증명 가능한 새로운 Feistal 구조를 제안했다. 제안된 구조는 다중 optimal diffusion 행렬에 대한 switching 기법을 이용한다. 즉, optimal diffusion 행렬들은 사전에 정해진 순서에 따라 각각의 라운드에 반복적으로 사용된다. 제안된 optimal diffusion 행렬들에 대한 switching기법을 DSM(Diffusion Switching Mechanism)이라 한다. [8]에서는 DSM의 효과에 대한 이론적인 분석이 처음으로 제시되었고, 또한 전체 라운드에서 능동 S 박스의 최소 개수를 계산하였다. 이는 능동 S 박스의 개수가 높을수록 Feistal 구조에서 확산 효과를 극대화하기 때문에 차분 공격과 선형 공격에 대한 안전성을 증명할 수 있다. 그러나 제안된 구조에 대한 행렬의 optimality 조건은 실제 블록 암호에 적용 가능한 행렬들을 찾기 어려운 제약 조건이다. [10]에서는 diffusion mapping에 대한 조건을 제거하고 일반적인 행렬을 적용한 DSN 설계 원리가 제안되었다. 이 구조는 행렬들에 대한 branch number가 알려졌을 경우 능동 S 박스의 최소 개수를 계산할 수 있다.

본 논문에서는 이진 행렬을 이용하여 DSM을 적용할 경우 주어진 optimality 조건을 만족하는 행렬은 존재하지 않음을 증명한다. 이는 이진 행렬을 이용하여 Shirai 등이 제안한 구조를 설계할 수 없음을 의미한다.

본 논문의 구성은 다음과 같다. 2절에서 Feistel 구조에서 DSM 설계 원리를 소개한고 3절에서는 이진 행렬을 적용하였을 경우의 증명을 제시하고 마지막으로 4절에서 본 논문의 결론을 맺는다.

2. DSM 설계 원리

본 절에서는 [9]에서 제안된 DSM 설계 원리를 소개하기 전에 증명에 사용되는 표기법과 개념들에 대해서 정의한다.

정의 1. b,r,k를 블록 암호 E의 블록 사이즈, r을 전체 라운드 수, k를 라운드키의 크기라고 정의할 때, $1 \leq i \leq r$에 대해, $k_i \in \{0,1\}^k$를 키스케쥴 함수로부터 생성된 라운드키로 표기하고 $x_i \in \{0,1\}^{b/2}$를 블록 암호 E의 중간값으로 표기한다. 라운드 함수에 사용되는 F 함수를 $F_i : \{0,1\}^{b/2} \times \{0,1\}^k \rightarrow \{0,1\}^{b/2}$로 정의하면 블록 암호 E의 balanced Feistel 알고리즘은 다음과 같이 정의된다.

1. 평문 $x_0, x_1 \in \{0,1\}^{b/2}$을 입력한다.
2. 중간값 $x_{i+1} = F_i(x_i, k_i) \oplus x_{i-1} (1 \leq i \leq r)$.
3. 암호문 $x_r, x_{r+1} \in \{0,1\}^{b/2}$.

라운드 함수에 사용되는 특별한 형태의 $SP-type$ F 함수를 다음과

* 본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음(IITA-2008-(C1090-0801-0025))

같이 정의한다.

정의 2. S 함수를 mn-비트의 입력값에 m 개의 n-비트 S 박스를 병렬로 적용하는 함수이고 P 함수를 mn-비트의 입력값과 출력값을 갖는 치환 함수일 때, i 번째 라운드의 $SP-type$ F 함수는 $F_i(x_i,k_i)=P_i(S_i(x_i \oplus k_i))$로 정의된다. 여기서 mn은 블록 길이의 $1/2$이며 x_i와 k_i의 길이는 $b/2$-비트이다.

정의 3. $(m,n,r)-SPFS$는 m개의 n-비트 S 박스를 사용하는 $SP-type$ 라운드 함수로 구성된 r-라운드 Feistel 구조로 정의한다.

정의 4. 벡터 $x=(x_0,x_1,...,x_{m-1}) \in GF(2^n)^m$의 해밍 웨이트 $w_n(x)$는 다음과 같이 정의된다.

$$w_n(x)=\#\{x_i \mid x_i \neq 0,\ 1 \le i \le m\}.$$

정의 5. 치환 함수 $P: \{0,1\}^{pn} \rightarrow \{0,1\}^{qn}$의 branch number $Br_n(P)$는 다음과 같다.

$$Br_n(P)=\min_{x \neq 0}\{w_n(x)+w_n(P(x))\}.$$

$Br_8(P)$는 0이 아닌 모든 입력 벡터 x에 대하여 x의 해밍 웨이트와 $P(x)$의 해밍 웨이트의 합 중에서 가장 작은 수를 의미한다. 예를 들어, $Br_8(P)=5$인 P에 대하여 입력 벡터중 0이 아닌 바이트가 1개라면 출력값에서 0이 아닌 바이트가 적어도 4개 이상 존재함을 의미한다. 동일하게 $Br_1(P)$는 0이 아닌 입력 비트와 출력 비트의 합 중에서 가장 작은 수를 의미한다.

정의 6. $GF(2^n)$에서 $p \times q$ 행렬 P에 대한 최대 branch number는 $Br_n(P)=q+1$이며, $m \times m$ 이진 행렬 P에 대한 최대 branch number $Br_1(P)$는 표 1.과 같다. 만약, 선형 변환 함수 P가 최대 branch number를 가질 경우 P를 optimal diffusion mapping이라 한다.

m	최대 branch number
3	3
4,5,6,7	4
8	5
9,10	6
11,13	7
12,14,15,...,26	8
27,28	9
29,30	10
31	11
32,33,34	12

표 1. $m \times m$ 이진 행렬의 최대 branch number

정의 7. m은 양의 정수이고 A, B는 $m \times m$ 정방 행렬일 때, $[A|B]$를 A와 B를 연접시킨 $m \times 2m$ 행렬이라 표기한다. 동일하게 세 개의 정방 행렬을 연접시켜 얻은 $m \times 3m$ 행렬을 $[A|B|C]$로 표기한다.

현재 블록 암호에서 능동 S 박스의 최소값은 차분 공격과 선형 공격에 대한 안전성으로 평가받는다. 이는 능동 S 박스의 개수가 주어진 차분과 선형 특성식의 확률값에 영향을 주기 때문이다. Shirai 등은 [9]에서 Feistel 구조에 optimal diffusion 행렬을 이용한 DSM 설계 원리를 제안하였다. Feistel 구조에서 DSM 설계 원리는 적어도 세 개의 다른 optimal diffusion 행렬들이 필요하며, 각 행렬들은 사전에 정해진 순서에 따라 각각의 라운드에 반복적으로 사용된다. $2r$-라운드 Feistel 구조에서 DSM 설계 원리와 필요한 optimality 조건은 다음과 같다.

1. 다음의 조건을 만족하는 $m \times m$ optimal diffusion 행렬 A_0, A_1, A_2을 선택한다.
   (a) $Br_n[A_0|A_1|A_2]=m+1$ $(n \ge 2)$,
   $Br_1[A_0|A_1|A_2]$는 A_j의 최대 branch number를 갖는다.
   (b) $Br_n[(A_0^{-1})^t|(A_1^{-1})^t]=Br_n[(A_1^{-1})^t|(A_2^{-1})^t]=$
   $Br_n[(A_2^{-1})^t|(A_0^{-1})^t]=m+1$ $(n \ge 2)$,
   $Br_1[(A_0^{-1})^t|(A_1^{-1})^t]=Br_1[(A_1^{-1})^t|(A_2^{-1})^t]=$
   $Br_1[(A_0^{-1})^t|(A_2^{-1})^t]$는 A_j의 최대 branch number를 갖는다.
2. 행렬 $A_{i \bmod 3}$을 $2i+1$ 번째 라운드의 치환 함수로 적용한다.
3. 행렬 $A_{i \bmod 3}$을 $2r-2i$번째 라운드의 치환 함수로 적용한다.

[8,10]에서는 이와 같이 Fistel 구조에 DSM 설계 원리를 적용했을 때 특정 라운드에서 능동 S 박스의 최소값을 계산할 수 있는 정리를 제시하였다.

정리 1. E는 $(m,n,r)-SPFS$ 블록 암호이다$(r \ge 6)$.
$[A_i|A_{i+2}|A_{i+4}]$와 $[(A_j^{-1})^t|(A_{j+2}^{-1})^t]$이 각각 optimal diffusion mapping일 때$(1 \le i \le r-4,\ 1 \le j \le r-2)$, 블록 암호 E의 임의의 연속적인 $3R$-라운드에서 차분과 선형 능동 S 박스의 개수는 적어도 $R(m+1)$이다$(R \ge 2)$.

DSM 설계 원리는 각각의 optimal diffusion 행렬들을 이용하며 이들을 연접한 행렬 역시 optimal diffusion mapping을 만족해야 한다. 그러나 이러한 조건은 실제 블록 암호에 적용하기 굉장히 어려운 조건이다. [10]에서 Shirai 등은 위의 optimality 조건을 만족하는 $GF(2^8)$의 8×8 행렬을 찾지 못하였다. 다음 절에서는 optimality 조건을 만족하는 $GF(2)$에서의 행렬은 존재하지 않음을 증명하겠다.

3. 연접된 이진 행렬의 최대 branch number 증명

본 절에서는 이진 행렬을 이용하여 DSM을 설계 원리를 적용할 경우 주어진 optimality 조건을 만족시키는 이진 행렬은 존재하지 않음을 증명한다. 증명은 $3 \le m \le 34$ 까지 각각 최대 branch number를 갖는 3개의 $m \times m$ 행렬을 연접한 이진 행렬 $[A_0|A_1|A_2]$의 branch number는 optimality 조건에 주어진 최대 branch number보다 작음을 보인다.

가. $m=3$, $Br_1[A_0|A_1|A_2]<3$

증명) 각 행렬은 branch number가 3이므로 하나의 열벡터의 해밍 웨이트는 2이상이다. 만일 모든 열벡터의 해밍 웨이트가 1이하라면 해

밍 웨이트가 1인 벡터 x에 대해 $A_j(x)$의 해밍 웨이트가 1로 계산되기 때문에 모순이 발생한다. 따라서 전체 행렬의 각 열에 올 수 있는 경우의 수는 4가지이다(=$\binom{3}{2}+\binom{3}{3}$). 그러나 3개의 연접된 행렬에 9개의 열이 존재하므로 동일한 두 열벡터가 반드시 존재한다. 동일한 두 열벡터에 대응하는 비트를 1로 고정하고 나머지 열멕터에 대응하는 비트가 모두 0인 입력 벡터 x에 대해서 출력값 $[A_0|A_1|A_2](x)$는 0이고 branch number는 2로 계산된다. 그러므로 $Br_1[A_0|A_1|A_2]$은 3보다 작고 최대값 2를 갖는다.

나. $4 \le m \le 8$, $\begin{cases} m=4,5,6,7 & \rightarrow Br_1[A_0|A_1|A_2] < 4 \\ m=8 & \rightarrow Br_1[A_0|A_1|A_2] < 5 \end{cases}$

증명) 전체 열의 개수는 $3m$이고, $3m$개의 열벡터 중에서 동일한 두 열벡터는 존재하지 않는다고 가정한다. 만일 동일한 두 열벡터가 존재한다면 **가.** 에서 보인 것과 같이 $[A_0|A_1|A_2](x)$이 0이 되는 벡터 x가 존재하게 된다. 전체 $3m$개의 열벡터 중에서 2개를 선택하는 경우의 수는 $\binom{3m}{2}$이다. 각각의 $m=4,...,8$에 대하여 $\binom{3m}{2} > 2^m$이 성립한다. 이는 임의의 2개의 열벡터를 선택하여 XOR 했을 때 결과값이 동일한 열벡터가 반드시 존재함을 의미한다. 세 열벡터에 대응하는 비트를 모두 1로 고정하고 나머지 비트가 모두 0인 입력 벡터 x에 대해서 $[A_0|A_1|A_2](x)$는 0이고 branch number는 3으로 계산된다.

따라서 $m=4,...,8$에 대하여 최대 branch number는 3이하다.

다. $9 \le m \le 13$, $\begin{cases} m=9,10 & \rightarrow Br_1[A_0|A_1|A_2] < 6 \\ m=11,13 & \rightarrow Br_1[A_0|A_1|A_2] < 7 \\ m=12 & \rightarrow Br_1[A_0|A_1|A_2] < 8 \end{cases}$

증명) 전체 열의 개수는 $3m$이고, 마찬가지로 같은 값을 갖는 두 열벡터는 존재하지 않는다고 가정한다. 전체 $3m$개의 열벡터 중에서 3개를 선택하는 경우의 수는 $\binom{3m}{3}$이다. 각각의 $m=9,...,13$에 대하여 $\binom{3m}{3} > 2^m$이 성립한다. 이는 임의의 3개의 열을 선택하여 XOR 했을 때 결과값이 동일한 열이 반드시 존재함을 의미한다.

따라서 $m=9,...,13$에 대하여 최대 branch number는 4이하다.

라. $14 \le m \le 18$, $Br_1[A_0|A_1|A_2] < 8$

증명) 전체 열의 개수는 $3m$이고, 마찬가지로 같은 값을 갖는 두 열벡터는 존재하지 않는다고 가정한다. 전체 $3m$개의 열벡터 중에서 4개를 선택하는 경우의 수는 $\binom{3m}{4}$이다. 각각의 $m=14,...,18$에 대하여 $\binom{3m}{4} > 2^m$이 성립한다. 이는 임의의 4개의 열을 선택하여 XOR 했을 때 결과값이 동일한 열이 반드시 존재함을 의미한다.

따라서 $m=14,...,18$에 대하여 최대 branch number는 5이하다.

마. $19 \le m \le 23$,, $Br_1[A_0|A_1|A_2] < 8$

증명) 전체 열의 개수는 $3m$이고, 마찬가지로 같은 값을 갖는 두 열벡터는 존재하지 않는다고 가정한다. 전체 $3m$개의 열벡터 중에서 5개를 선택하는 경우의 수는 $\binom{3m}{5}$이다. 각각의 $m=19,...,23$에 대하여 $\binom{3m}{5} > 2^m$이 성립한다. 이는 임의의 5개의 열을 선택하여 XOR 했을 때 결과값이 동일한 열이 반드시 존재함을 의미한다.

따라서 $m=19,...,23$에 대하여 최대 branch number는 6이하다.

바. $24 \le m \le 28$, $\begin{cases} m=24,25,26 & \rightarrow Br_1[A_0|A_1|A_2] < 8 \\ m=27,28 & \rightarrow Br_1[A_0|A_1|A_2] < 9 \end{cases}$

증명) 전체 열의 개수는 $3m$이고, 마찬가지로 같은 값을 갖는 두 열벡터는 존재하지 않는다고 가정한다. 전체 $3m$개의 열벡터 중에서 7개를 선택하는 경우의 수는 $\binom{3m}{6}$이다. 각각의 $m=29,...,34$에 대하여 $\binom{3m}{6} > 2^m$이 성립한다. 이는 임의의 6개의 열을 선택하여 XOR 했을 때 결과값이 동일한 열이 반드시 존재함을 의미한다.

따라서 $m=24,...,28$에 대하여 최대 branch number는 7이하다.

사. $29 \le m \le 34$, $\begin{cases} m=29,30 & \rightarrow Br_1[A_0|A_1|A_2] < 10 \\ m=32 & \rightarrow Br_1[A_0|A_1|A_2] < 11 \\ m=32,33,34 & \rightarrow Br_1[A_0|A_1|A_2] < 12 \end{cases}$

증명) 전체 열의 개수는 $3m$이고, 마찬가지로 같은 값을 갖는 두 열벡터는 존재하지 않는다고 가정한다. 전체 $3m$개의 열벡터 중에서 7개를 선택하는 경우의 수는 $\binom{3m}{7}$이다. 각각의 $m=29,...,34$에 대하여 $\binom{3m}{7} > 2^m$이 성립한다. 이는 임의의 7개의 열을 선택하여 XOR 했을 때 결과값이 동일한 열이 반드시 존재함을 의미한다.

따라서 $m=29,...,34$에 대하여 최대 branch number는 8이하다.

4. 결 론

본 논문에서는 Feistal 구조에 DSM 설계 원리를 적용하기 위해 필요한 optimality 조건을 만족하는 $m \times m$ 이진 행렬은 존재하지 않음을 증명했다. 증명은 세 개의 optimal diffusion 행렬들의 연접된 행렬은 각 행렬의 최대 branch number를 갖지 못함을 보였다. 현재까지 $GF(2^n)$에서 DSM 설계 원리의 optimality 조건을 만족하는 행렬은 발견하지 못하였다. 향후 $GF(2^n)$에서 optimality 조건을 만족하는 행렬의 존재성 연구와 함께 DSM 설계 원리에 적합한 행렬에 대한 연구가 요구된다.

참 고 문 헌

[1] P. Barreto and V. Rijmen, "The Whirlpool hasing function, Primitive submitted to NESSIE, 2000",
http://www.cryptonessie.org/.

[2] E. Biham and A. Shamir, "Differential Cryptanalysis of DES-like Cryptosystems", Journal of Cryptology, Vol. 4, NO. 1, pp. 3-72, 1991.

[3] J. Daemen and V. Rijmen, "The Designe of Rijndael: AES-The Advanced Encryption Standard", (Information Security and Cryptography), Springer, 2002.

[4] M. Matsui, "The First Experimental Cryptanalysis of the Data Encryption Standard", CRYPTO'94, LNCS 839, pp. 1-11, Springer-Verlag, 1994.

[5] V. Rijmen, J. daemen, B. Preneel, A. Bossalaers and E. Win, "The Cipher SHARK", FSE'96, LNCS 1039, pp. 99-101, Springer_Verlag , 1996.

[6] B. Schneier, J. kelsey, D. Whiting, D. Wagner, C. Hall and N. Ferguson, "Two fish: A 128-bit block cipher", Primitive submitted to AES, 1998, http://www.schneeier.com/

[7] C. E. Shannon, "Communications Theory of Secrecy System". Bell System Technical journal, Vol. 28, NO. 4, pp. 656-751, 1949.

[8] T. Shirai and B. Preneel, "On Feistel Ciphers Using Optimal Diffusion Mappings Across Multiple Rounds", ASIACRYPT'04, LNCS 3329, Springer-Verlag, pp. 1-15. 2004.

[9] T. Shirai and K. Shibutani, "Improving Immunity of Feistel Ciphers against Differential Cryptanalysis by Using Multiple MDS Matrices", FSE'04, LNCS 3017, pp. 260-278, Springer-Verlag, 2004.

[10] T. Shirai and K. Shibutani, "On Feistel Structures Using a Diffusion Switching Mechanism", FSE'06, LNCS 4047, pp. 41-56 Springer-Verlag, 2006.