DBpia

論文 95-2-2-4

PN시퀀스를 이용한 S-box 설계에 관한 연구

正會員 崔 會 東*, 正會員 盧 宗 善**

A Study on S-box Design by Using PN Sequences

Hoi-Dong Cho*, Jong-Seon No**, Regular Members

要 約

대치 암호 방법은 과거로부터 널리 사용되어온 암호화 방식의 하나이다. S-box는 이러한 대치 암호 방식에서 사용되며 또한 DES에서는 매우 중요한 요소로서 사용되고 있다. 본 논문에서는 일반적인 m시퀀스 $tr_m^n(\alpha^t)$를 이용하여 새로운 S-box를 설계 하는 알고리듬을 제안하였다. 여기서 $tr_m^n(\alpha^t)$는 GF(2^n)에서 GF(2^m)로 선형 매핑이다. n=16과 m=4의 경우에 대한 모의실험 결과, 제안된 S-box 알고리듬은 DES의 S-box보다 SAC와 출력 비트 간의 상관관계가 매우 우수함이 증명되어 안전성이 입증되었다. 그러나 제안된 알고리듬은 차이 암호분석과 선형 암호분석 등의 방법을 이용한 공격에 대해서 더 많은 연구가 필요하다.

ABSTRACT

Substitution cipher is one of the popular cryptosystems that have been world-widely used long ago. S-box is used in the substitution cipher and in DES as the most important component. In this paper, algorithms that generate new S-boxes using the generalized m sequence $tr_m^n(\alpha^t)$, that linearly maps GF(2^n) intoGF(2^m), are proposed. From the simulation result in case of n=16 and m=4, it is shown that the proposed S-box algorithms have better SAC and correlation properties between output bits than that of the S-box of DES. However, the proposed algorithms are required further research about cryptanalytic attacks using the differential cryptanalysis and the linear cryptanalysis.

Ⅰ. 서 론

통신시스템이 점점 발달함에 따라 통화도용, 도청, 불법적인 통신사기 등에 의해 기업 및 국가의 비밀정보의 부정 유출, 전송되는 정보의 변조 등 엄청난 해악을 가져다 줄 것으로 우려되고 있다. 이러한 역기능을 막기 위해서 암호시스템의 필요성이 최근 들어서 증대되고 있다.

S-box를 요소기술로 사용하고 있는 DES(Data Encryption Standard)는 IBM에서 Lucifer 시스

*현대전자 CDMA 시스템 사업단
**건국대학교 전자공학과
Dept. of Electronic Eng. Konkuk Univ.
論文番號 : 94214
接受日字 : 1994年 8月 6日

www.dbpia.co.kr

템을 개선하여 개발한 암호시스템으로, 1977년 미국 상무성의 국립 표준국(National Bureau of Standard, NBS)에서 미국 표준 암호알고리듬으로 채택한 64비트 블럭의 입력 및 출력을 가지는 블럭 암호시스템이다[1].

DES의 안전성은 비선형인 S-box 테이블의 특성분석으로 SAC(Strict Avalanche Criterion) 분석 방법과 출력 비트간의 상관관계를 구하는 방법이 있다.

Kam과 Davida[2]가 완전성(completeness)을, Feistel[3]이 애벌런치 효과(avalanche effect)를 각각 처음으로 소개했고, Webster와 Tavares[4]는 완전성과 애벌런치 효과를 결합하여 SAC을 정의했다. 또한 애벌런치 벡터의 각 비트간의 상관계수를 구하여 상호 상관관계 정도를 결정하는 출력 비트간의 상관관계도 정의했다.

Biham과 Shamir[5]가 발표한 차이 암호분석(differential cryptanalysis)은 두 평문의 XOR가 특정한 값을 갖고 입력될 때 이에 대응하여 발생되는 암호문 쌍은 높은 확률의 XOR값으로 발생되는데 기초를 둔 선택평문 공격(chosen-plaintext attack) 방법이다. 이 들은 DES와 관용 암호시스템을 쉽게 공격할 수 있는 공격 방법으로 주목받고 있다.

선형 암호분석(linear cryptanalysis)[6]은 Matsui가 발표한 DES에 관한 새로운 해독 방법이다. 암호 알고리듬에 대하여 그 평문과 암호문의 관계를 비트 단위로 선형근사를 시킨다. 이 근사식을 암호함수에서부터 알고리듬 전체로 확장하고, 최종적으로 평문으로부터 암호문에 이르는 일련의 확률적 선형 비트 경로를 구성하여 그 경로에 영향을 주는 키 비트를 높은 확률로 추정한 후 나머지 키 비트를 exhaustive공격으로 구하는 방법이다.

본 논문은 램덤과 유사한 특성을 지닌 PN시퀀스를 사용하여 새로운 S-box를 설계하는 알고리듬을 제안하였고 이 새로운 S-box 알고리듬에 대하여 SAC와 출력 비트간의 상관관계, 차이 암호분석 공격에 이용되는 입력 XOR와 출력 XOR의 분포도, 그리고 선형 암호분석 공격에 이용되는 입력비트 위치와 출력비트 XOR값이 일치하는 경우의 수에 대한 테이블을 작성하여 DES의 S-box와 비교하였다. Ⅱ장에서는 PN시퀀스를 이용한 3가지의 새로운 S-box를 설계하는 알고리듬을 제안한다. Ⅲ장은 DES의 S-box와 제안한 알고리듬에 의한 S-box 대한 SAC와 출력 비트간의 상관관계를 이용한 안전성을 비교 분석 하였다.

Ⅱ. PN시퀀스에 의한 S-box 발생

2.1 PN시퀀스의 발생

n단으로 구성된 선형궤환시프트레지스터(LFSR)에서 최대로 가능한 발생 주기가 2^n-1인 시퀀스를 최대 LFSR 시퀀스 또는 m시퀀스라 부른다.

본 논문에서 사용하는 일반적인 m시퀀스(generalized m-sequences)는 GF(2^n)으로부터 GF(2^m)으로의 매핑과정이고, $tr_m^n(\alpha^i)$는 GF(2^m)의 원소를 가지는 m시퀀스이다. 여기서 n=16, m=4를 가정하자. 그러면 일반적인 m시퀀스를 발생시키기 위하여 다음의 사항이 필요하다.

- 주기는 $N=2^{16}-1=65535$ 이다.
- 사용된 α의 원시다항식(primitive polynomial)은
  $M_\alpha(x)=x^{16}+x^{12}+x^3+x+1$ (3)
  이다.
- GF(2)에서 β의 최소다항식은
  $M_\beta=x^4+x+1$ (4)
  이다. 여기서 $\beta=\alpha^{2^n+1}$이다.

2.2 PN시퀀스를 이용한 새로운 S-box 제안

본 논문에서는 매우 긴 주기로 램덤과 유사한 특성을 지니는 PN시퀀스를 이용하여 DES의 S-box에 대해 그림 1처럼 GMS(Generalized M-Sequences)1, GMS2, GMS3 등의 3가지 새로운 S-box 생성 알고리듬을 제안한다.

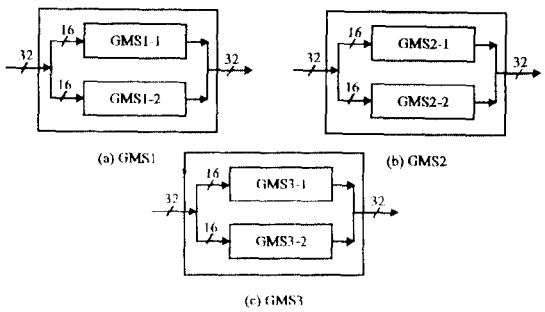


그림 1. 제안된 S-box 알고리듬
Fig. 1. Proposed S-box algorithm

www.dbpia.co.kr

제안한 알고리듬들을 발생시키는 순서는 다음 절에 있다. DES가 16라운드이므로 클럭을 16번 가하는 것으로 한다. 그러나 제안된 m시퀀스의 단점은 모두 0으로 구성된 입력을 사용하면 계속해서 0이 발생된다는 것이다.

2.2.1 GMS1

그림 2는 일반적인 m시퀀스(GMS) 발생기를 이용한 S-box로 16비트 입력과 16비트 출력을 갖는다. 그리고 $\beta_i = \beta^{i-1}(i=0,1,2,3)$이다.

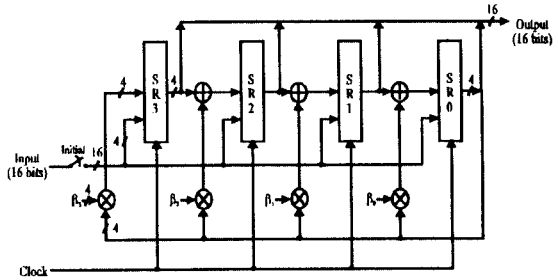


그림 2. 일반적인 m시퀀스를 이용한 GMS1
Fig. 2. GMS1 using generalized m-sequences

이 알고리듬은 클럭을 16번 가하며, 매 클럭마다 일반적인 m시퀀스 발생 알고리듬에 따라 각 레지스터 값이 변한다.

선형궤환쉬프트레지스터의 두 배인 2n개의 시퀀스를 알면 n개의 선형방정식을 해석하여 다음 상태를 알 수 있다. 그러므로 이 알고리듬은 선형적이라고 할 수 있다.

2.2.2 GMS2

이 알고리듬은 그림 3과 같이 일반적인 m시퀀스를 이용하여 16비트 입력과 16비트 출력을 갖는다.

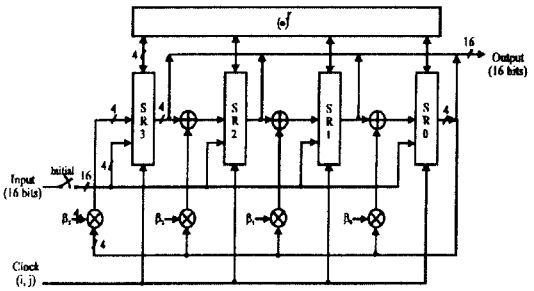


그림 3. 일반적인 m시퀀스를 이용한 GMS2
Fig. 3. GMS2 using generalized m-sequences

여기서 γ는 다음과 같은 식을 만족한다.

$$g.c.d(2^{16}-1,\gamma)=1 \quad (5)$$

처음 클럭은 8번 가하고, 각 선형궤환쉬프트레지스터의 내용을 함수$(\cdot)^{\gamma}$에 보내어 γ제곱을 하고 다시 각각 선형궤환쉬프트레지스터로 보낸다. 그리고 다음 클럭은 8번 가한다.

이 알고리듬은 GMS1의 단점인 선형의 성질을 해결하기 위해 함수$(\cdot)^{\gamma}$를 사용하여 비선형 구조를 갖게 한다. 여기서 γ제곱은 16-tuple이다.

2.2.3 GMS3

그림 4에서는 16비트 입력과 16비트 출력을 발생시키는데 일반적인 m시퀀스를 이용한다.

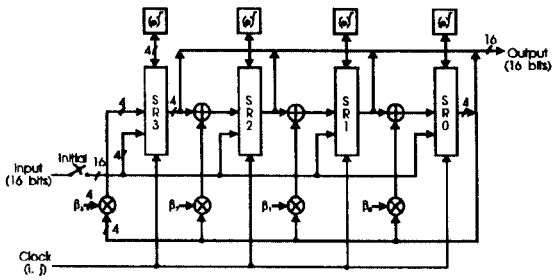


그림 4. 일반적인 m시퀀스를 이용한 GMS3
Fig. 4. GMS3 using generalized m-sequences

여기서 γ는 다음과 같은 식을 만족한다.

$$g.c.d(2^{4}-1,\gamma)=1 \quad (6)$$

처음 클럭은 8번 가하고, 각각 선형궤환쉬프트레지스터 내용을 함수$(\cdot)^{\gamma}$에 보내어 γ제곱을 하고, 다시 각각 선형궤환쉬프트레지스터에 보낸다. 그리고 다음 클럭은 8번 가한다.

이 알고리듬은 각각 선형궤환쉬프트레지스터의 내용을 4-tuple의 γ제곱하여 비선형 구조를 갖게 한다.

Ⅲ. DES의 S-box와 제안된 S-box와의 안전성 비교 및 분석

S-box에 대한 안전성 평가는 SAC 분석 방법과 출력 비트간의 상호의존도를 평가하는 상관계수 방법을 이용한다.

그리고 DES와 유사한 대칭키 반복 암호 알고리듬은 차이 암호분석(differential cryptanalysis) 및

www.dbpia.co.kr

선형암호분석(linear cryptanalysis) 공격 방법 등이 있다.

3.1 SAC의 분석

두개의 n비트 평문 벡터 X와 비트 i가 다른X_i에 대해 애벌런치 벡터를 고려해 보자.

$$V_i=Y\oplus Y_i \quad (7)$$

여기서 $Y=f(X)$, $Y_i=f(X_i)$, f는 암호화 함수, $1\le i\le n$이다.

SAC 관계식은 다음과 같다.

$$\sum_{X\in Z_2^n}[f(X)\oplus f(X_i)]=S \quad (8)$$

여기서 Z_2^n은 GF(2)상에서의 n차원 벡터 스페이스이고, S는 (V_{ji}), 그리고 $1\le j\le m$, $1\le i\le n$이다.

(1) DES의 S-box

각 S-box는 6비트 입력과 4비트 출력으로 구성된다.

모든 입력 벡터들에 대해 출력 벡터의 SAC 확률 P_{ij}가 0.5일 때가 가장 이상적이다. 여기서 i는 입력 벡터의 비트이고 j는 출력 벡터의 비트이다.

표 1은 DES의 S-box들에 대한 각 평균이다. 이들 평균은 0.6146에서 0.6641 사이의 값을 갖는다.

표 1. DES의 S-box들에 대한 확률 평균
Table 1. Average of SAC for S-boxes of DES

DES	평균
S-box1	0.6198
S-box2	0.6328
S-box3	0.6641
S-box4	0.6146
S-box5	0.6328
S-box6	0.6484
S-box7	0.6563
S-box8	0.6250

(2) GMS1

GMS1-1의 원시원은 6029, GMS1-2의 원시원은 241을 사용하고 클럭은 16번을 가한다.

표 2는 GMS1의 SAC 확률 평균이다. 이때 GMS1-1의 총 평균은 0.4852, GMS1-2의 총 평균은 0.4881이다.

(3) GMS2

이 알고리듬은 GMS2-1의 원시원을 14011, GMS2-2의 원시원을 4967로 사용하고, 처음 클럭은 8번을 가한다. 그리고 GMS2-1의 γ제곱은 311, GMS2-2의 γ제곱은 5791을 사용하며 다음 클럭은 8번을 가한다.

표 2. GMS1의 SAC 확률 평균
Table 2. Average of SAC for GMS1

입력 (i)	출력(j)의 평균		입력 (i)	출력(j)의 평균	
	GMS1-1	GMS1-2		GMS1-1	GMS1-2
2	0.4867	0.4874	10	0.4853	0.4871
3	0.4860	0.4907	11	0.4785	0.4888
4	0.4931	0.4896	12	0.4820	0.4877
5	0.4889	0.4889	13	0.4821	0.4882
6	0.4856	0.4885	14	0.4838	0.4856
7	0.4839	0.4896	15	0.4777	0.4879
8	0.4891	0.4874	16	0.4851	0.4847
9	0.4901	0.4895	총 평균	0.4852	0.4881

표 3에서 i는 입력 벡터의 비트 위치, j는 출력 벡터의 비트 위치이고 입력 벡터와 출력 벡터의 상관관계를 구한 것이다. GMS2-1의 총 평균은 0.4916, GMS2-2의 총 평균은 0.4836이다.

표 3. GMS2의 SAC 확률 평균
Table 3. Average of SAC for GMS2

입력 (i)	출력(j)의 평균		입력 (i)	출력(j)의 평균	
	GMS2-1	GMS2-2		GMS2-1	GMS2-2
2	0.4925	0.4834	10	0.4928	0.4849
3	0.4912	0.4826	11	0.4932	0.4840
4	0.4913	0.4837	12	0.4899	0.4834
5	0.4921	0.4846	13	0.4946	0.4831
6	0.4903	0.4830	14	0.4922	0.4844
7	0.4918	0.4806	15	0.4920	0.4856
8	0.4896	0.4861	16	0.4887	0.4845
9	0.4917	0.4798	총 평균	0.4915	0.4836

표 4. GMS3의 SAC 확률 평균
Table 4. Average of SAC for GMS3

입력 (i)	출력(j)의 평균		입력 (i)	출력(j)의 평균	
	GMS3-1	GMS3-2		GMS3-1	GMS3-2
2	0.4887	0.4939	10	0.4896	0.4910
3	0.4889	0.4922	11	0.4897	0.4921
4	0.4864	0.4929	12	0.4862	0.4913
5	0.4873	0.4926	13	0.4887	0.4982
6	0.4895	0.4943	14	0.4879	0.4941
7	0.4863	0.4937	15	0.4871	0.4912
8	0.4877	0.4913	16	0.4849	0.4916
9	0.4891	0.4947	총 평균	0.4879	0.4930

(4) GMS3

이 알고리듬은 GMS3-1의 원시원으로 4409, GMS3-2의 원시원으로 10171을 사용하고, 처음 클럭은 8번을 가한다. 그리고 GMS3-1과 GMS3-2의 γ제곱는 7을 사용며 다음 클럭은 8번을 가한다.

www.dbpia.co.kr

표 4는 GMS3의 각 입력 i에 대해 출력 j의 평균이다. 이때 GMS3-1의 총 평균은 0.4879, GMS3-2의 총평균은 0.4930이다.

(5) SAC 분석 결과

그림 5은 DES의 S-box와 제안된 S-box의 SAC에 대한 비교 그림이다. 가장 이상적인 SAC는 0.5이다.

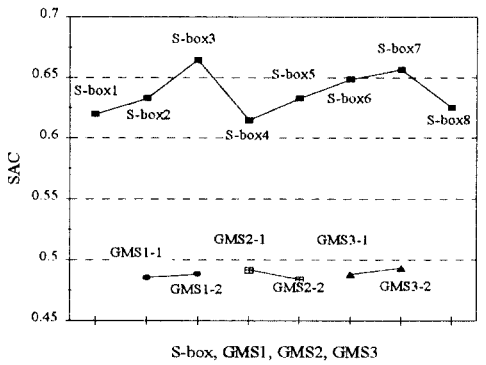


그림 5. DES의 S-box와 제안된 S-box의 SAC 비교
Fig 5. The comparision of SAC between S-boxes of DES ans proposed S-boxes

3.2 출력 비트간의 상관계수

모든 가능한 입력 벡터에 대해 각 출력 비트간의 상관계수의 계산식은 다음과 같다.

$$\rho_{ij}(x)=\frac{\mathrm{cov}(i,j)}{\sigma(i)\cdot\sigma(j)} \tag{9}$$

여기서 x는 입력 벡터의 비트 위치이고, i와 j는 출력 벡터의 비트 위치이다.

(1) DES의 S-box

표 5는 DES의 S-box들에 대한 각 상관계수의 평균이다. 평균값들이 -0.1528에서 -0.2323내의 값들을 가지며, 비트간 상호독립이라 할 수 있다.

(2) GMS1

출력 비트간의 상관계수는 애벌런치 벡터의 각 비트간 상관계수를 구하여 비트간 상호 연관성을 알 수 있다.

일반적인 m시퀀스 발생 알고리듬에서 살펴보면, 쉬프트레지스터1의 다음 상태는 쉬프트레지스터2와 β_2결과의 XOR이므로 본 논문에서는 상관계수 $\rho_{ij}(x)$를

표 5. DES의 S-box들에 대한 각 상관계수 평균
Table 5. Each of average of correlation coefficients for S-boxes of DES

DES	평균
S-box1	-0.1952
S-box2	-0.1882
S-box3	-0.1611
S-box4	-0.2323
S-box5	-0.1842
S-box6	-0.1875
S-box7	-0.1528
S-box8	-0.1762

다음과 같은 방법으로 구하였다.

i=1, 2, 3, 4일 때, 이에 대해 각각 j=5, 6, 7, 8이고, i=5, 6, 7, 8일 때, 이에 대해 각각 j=9, 10, 11,12이고, i=9, 10, 11, 12일 때, 이에 대해 각각 j=13,14, 15, 16이다.

표 6은 입력 벡터의 비트 위치에 대한 상관계수의 평균이다. GMS1-1의 총 평균은 0.0140이고, GMS1-2의 총 평균은 0.0056이다.

표 6. GMS1의 입력 벡터의 비트 위치에 대한 평균
Table 6. Average of correlation coefficients for GMS1

입력 비트	출력의 평균		입력 비트	출력의 평균	
	GMS1-1	GMS1-2		GMS1-1	GMS1-2
2	0.0139	0.0030	10	0.0122	0.0071
3	0.0160	0.0040	11	0.0180	0.0062
4	0.0084	0.0061	12	0.0060	0.0039
5	0.0101	0.0059	13	0.0147	0.0085
6	0.0130	0.0036	14	0.0155	0.0083
7	0.0195	0.0063	15	0.0233	0.0074
8	0.0136	0.0048	16	0.0135	0.0066
9	0.0126	0.0027	총 평균	0.0140	0.0056

(3) GMS2

표 7은 입력 벡터의 비트 위치에 대한 상관계수의 평균이다. GMS2-1의 총 평균은 0.0107이고, GMS2-2의 총 평균은 0.0107이다.

(4) GMS3

표 8은 입력 벡터의 비트 위치에 대한 상관계수의 평균이다. GMS3-1의 총 평균은 0.0095이고, GMS3-1의 총 평균은 0.0043이다.

(5) 출력 비트간의 상관관계에 대한 분석 결과

그림 6은 DES의 S-box와 제안된 S-box의 출력비

www.dbpia.co.kr

표 7. GMS2의 입력 벡터의 비트 위치에 대한 평균
Table 7. Average of correlation coefficients for GMS2

입력	출력의 평균		입력	출력의 평균	
비트	GMS2-1	GMS2-2	비트	GMS2-1	GMS2-2
2	0.0096	0.0125	10	0.0095	0.0094
3	0.0111	0.0129	11	0.0114	0.0082
4	0.0132	0.0118	12	0.0129	0.0121
5	0.0124	0.0102	13	0.0057	0.0107
6	0.0086	0.0094	14	0.0084	0.0129
7	0.0118	0.0108	15	0.0109	0.0091
8	0.0134	0.0101	16	0.0133	0.0105
9	0.0080	0.0097	총 평균	0.0107	0.0107

표 8. GMS3의 입력 벡터의 비트 위치에 대한 평균
Table 8. Average of correlation coefficients for GMS3

입력	출력의 평균		입력	출력의 평균	
비트	GMS3-1	GMS3-2	비트	GMS3-1	GMS3-2
2	0.0102	0.0058	10	0.0088	0.0039
3	0.0112	0.0029	11	0.0087	0.0056
4	0.0109	0.0035	12	0.0106	0.0082
5	0.0077	0.0076	13	0.0097	-0.0012
6	0.0075	0.0034	14	0.0068	0.0034
7	0.0099	0.0059	15	0.0083	0.0043
8	0.0118	0.0053	16	0.0124	0.0040
9	0.0087	0.0022	총 평균	0.0095	0.0043

트간 상관계수 비교 그림이다. $\rho_{ij}(x)$가 0일 때 비트간은 서로 상관관계가 없다.

3.3 차이 암호분석

동일한 암호함수에 입력되는 두 입력의 XOR와 출력 XOR의 분포도는 그림 7과 같은 방법으로 얻는다.

이러한 출력 값들이 균일하게 분포된 S-box 테이블을 사용하므로 입력에 대한 출력 값들의 발생 빈도수는 동일한 분포를 갖게 된다. 그러나 균일한 분포를 갖지 못하고 큰 분포를 갖는 입력 XOR에 대한 출력 XOR를 높은 확률로 예측하여 차이 암호분석 공격에 이용한다.

Biham과 Shamir는 차이 암호분석을 이용하여 8라운드는 2분내에 암호키를 찾아냈고[9], 16라운드에서 Exhaustive 공격 방법보다 빠르게 공격할 수 있다고 하였다[10].

표 9은 DES의 S-box에 대한 영이 아닌 요소의 평균과 최대 분포도이다.

본 논문는 65534개의 입력 XOR 중에서 랜덤하게

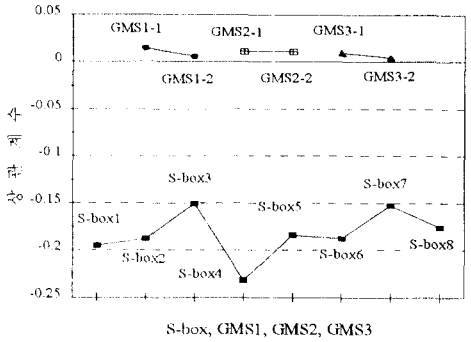


그림 6. DES의 S-box와 제안된 S-box의 상관계수 비교
Fig 6. The comparition of correlation coefficients between S-boxes of DES and proposed S-boxes

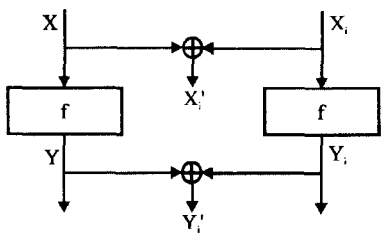


그림 7. 입력 XOR와 출력 XOR
Fig 7. Input XOR and out XOR

1000개에 대하여 모의 실험을 하였다.

각 알고리듬의 최대 분포와 영이 아닌 분포의 평균은 표 10와 같다.

표 9. DES의 S-box에 대한 영이 아닌 요소의 평균과 최대 분포도
Table 9. Average of nonzero element and maximal distribution for S-boxes of DES

DES	영이 아닌 요소의 평균	최대 분포
S-box1	79.49	16
S-box2	78.61	16
S-box3	79.69	16
S-box4	68.55	16
S-box5	76.56	16
S-box6	80.76	16
S-box7	77.25	16
S-box8	77.15	16

3.4 선형 암호분석

함수 f의 입력 비트 위치와 출력 비트 XOR값이 일치하는 경우의 수가 1/2에 근접하도록 함수를 설계하면 선형 암호분석 공격에 강해진다.

www.dbpia.co.kr

표 10. 각 알고리듬에서 최대 분포와 영이 아닌 분포의 평균
Table 10. Average of nonzero element and maximal distribution for proposed S-boxes

제안한 알고리듬		영이 아닌 분포의 평균	최대 분포
GMS1	GMS1-1	32.59	1180
	GMS1-2	36.40	176
GMS2	GMS2-1	36.34	1048
	GMS2-2	32.95	8206
GMS3	GMS3-1	36.30	258
	GMS3-2	32.68	524

표 11. DES의 S-box에 대한 최대 분산
Table 11. The maximal variance for S-boxes of DES

DES	최대 분산
S-box1	18
S-box2	16
S-box3	16
S-box4	16
S-box5	20
S-box6	14
S-box7	18
S-box8	16

표 11은 DES의 S-box에 대한 최대 분산을 나타내는 표이다.

제안한 알고리듬들의 입력 비트 위치와 출력 비트 XOR값이 일치하는 경우의 수에 대한 분산정도가 최대인 것은 표 12와 같고 이때 기준은 32767이다.

표 12. 제안한 알고리듬들에 대한 최대 분산
Table 12. The maximal variance for proposed S-boxes

제안한 알고리듬		최대 분산
GMS1	GMS1-1	736
	GMS1-2	657
GMS2	GMS2-1	504
	GMS2-2	639
GMS3	GMS3-1	497
	GMS3-2	505

3.5 분석 결과

선형궤환시프트레지스터가 16단인 일반적인 m시퀀스는 2048개의 서로 다른 시퀀스를 발생시킬 수 있다.

이중에서 63개에 대해 모의실험을 해보았다.

원시원이 5471와 6971일 때 SAC는 0.1177 이하이고, 출력 비트간 상관계수는 0.2685 이상으로 특성이 불량한 경우이다. 그러나 원시원이 361, 1081, 3899, 6029, 14011, 등 50개는 SAC가 0.4이상이고 출력 비트간 상관계수는 0.014이하로 특성이 우수한 경우이다.

GMS2는 원시원이 불량하면 γ제곱에 관계없이 SAC가 불량하다. 그러나 반대로 원시원이 우수하면 γ제곱에 관계없이 우수하다.

GMS3은 GMS2와 같은 결과를 갖지만 γ제곱에 사용할 수 있는 것은 1과 7뿐이다.

GMS2와 GMS3에서 비트간의 상관계수는 원시원이 불량이면 0.2이상을 갖지만, 원시원이 우수하면 0.02이하로 비트 간은 서로 독립이라 할 수 있다.

DES는 16라운드로 구성되어 있으므로 제안한 알고리듬에서 기본적으로 클럭을 16번 가해주는 것으로 모의실험을 하였다. 그러나 제안한 알고리듬은 적절한 클럭 수와 γ제곱을 비밀 키로도 사용할 수 있는 장점이 있다.

제안한 알고리듬에 대해 입력 XOR와 출력 XOR 분포 테이블, 입력 비트 위치와 출력 비트 XOR값이 일치하는 경우의 수에 대한 테이블을 구해 보았다. S-box는 64×16 테이블이지만 제안한 알고리듬은 65535×65535 테이블로 매우 복잡하다.

앞으로 이런 테이블을 이용하여 차이 암호분석과 선형 암호분석 공격에 대해 더 많은 연구가 필요하다.

Ⅳ. 결 론

정보통신기술의 발전과 더불어 부수적으로 발생하는 통화도용, 도청, 불법적인 통신사기 등의 역기능을 막기 위해서 암호의 필요성이 대두되고 있다.

PN시퀀스는 균형과 스팬 특성을 가지고 있어 매우 랜덤한 성질의 특성을 갖고 있는 것으로 간주된다.

표 13. DES의 S-box와 제안한 알고리듬에 대해 SAC와 상관계수의 비교
Table 13. The comparision between SAC and correlation coefficients for S-boxes of DES and proposed S-boxes

비교	SAC의 평균	상관계수의 평균
S-box	0.6367	-0.1846
GMS1	0.4866	0.0098
GMS2	0.4875	0.0107
GMS3	0.4904	0.0069

본 논문에서는 이러한 특성을 이용한 새로운 S-box 설계에 대한 알고리듬을 제안하고, DES의 S-

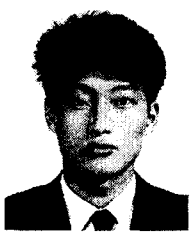
www.dbpia.co.kr

box와 제안된 S-box 알고리듬에 대해 SAC와 비트간의 상관관계를 모의실험으로 조사해 보았다. 그 결과 표 13처럼 SAC와 비트간의 상관관계가 매우 우수한 특성을 갖음을 증명하였다. 즉 제안한 알고리듬이 DES의 S-box보다는 높은 안전성을 갖는 것으로 분석되었다.

그러나 제안한 알고리듬은 차이 암호분석과 선형암호분석 등의 방법을 이용한 공격에 대해서 더 많은 연구가 필요하다.

참고문헌

1. National Bureau of Standards, "Data Encryption Standard," Federal Information Processing Standard(FIPS), Publication no. 46, Jan. 1977.
2. Kam, J. B., and Davida, G. I. : Structured Design of Substitution-Permutation Encryption networks. IEEE Transactions on Computers, Vol. 28, No. 10, 744(1979).
3. Feistel, H. : Cryptography and Computer Privary. Scientific American, Vol. 228, No. 5, 15(1973).
4. A. F. Webster and S. E. Tavares, "On the Design of Sboxes, Proc. of CRYPTO'85, Springer-Verlag, 1985.
5. E. Biham and A. Shamir, "Differential Cryptanalysis of DES-like Cryptosystems," Journal of CRYPTOLOGY, Vol. 4, No. 1, 1991.
6. M. Matsui, "Linear Cryptanalysis Method for DES Cipher," Proc. of SCIS'93, SCIS'93-3c, 1993.
7. S. W. Golomb, Shift Register Sequences. San Francisco, CA : Holden-Day, 1967 : revised edition, Laguna Hills, CA : Aegean Park Press, 1982.
8. J. S. No and P. V. Kumar, "A New Family of Binary Pseudorandom Sequences Having Optimal Periodic Correlation Properties and large Linear Span," IEEE Trans. Inform. Theory, Vol. IT-35, No. 2, pp. 371-379, March 1989.
9. E. Biham and A. Shamir. "Differential Cryptanalysis of DES-like Cryptosystems." in Proc. of Crypt'90, 1990.
10. E. Biham and A. Shamir. "Differential Cryptanalysis of the Full 16-rount DES." in Proc. of Crypt'92, 1992.
11. 한국전자통신연구소, "현대암호학," 1991 한국전자통신연구소



崔 會 東(Hoi Dong Choi) 정회원

1965년 5월 2일생

1992년 2월 : 건국대학교 공과대학 전자공학과(학사)

1994년 8월 : 건국대학교 공과대학 전자공학과 석사졸업

1994년 8월~현재 : 현대전자 CDMA 시스템 사업단

盧 宗 善(Jong Seon No) 정회원

현 재 : 건국대학교 전자공학과 조교수

제 18권 11호 참조.

www.dbpia.co.kr