通信情報保護學會論文誌
第 10 券 第 4 號, 2000. 12

블록 암호 알고리즘 HEA에 대한 차분분석

현 진 수*, 송 정 환*, 강 형 석**

Differential Cryptanalysis of DES-Like Block Cipher HEA

Jin Su Hyun*, Jung Hwan Song*, Hyung Suk Kang**

요 약

본 논문에서는 DES(Data Encryption Standard)를 변형하여 설계된 HEA(Hangul Encryption Algorithm)을 차분분석 관점에서의 안전성에 대하여 고찰하고자 한다. HEA는 한글 64음절(1,024 비트) 입·출력이 되도록 설계된 56비트 키를 사용하고 DES와 동일한 8개의 S-box를 적용한 16라운드 Fiestel 구조의 블록 암호알고리즘이다. 본 논문에서는 기존의 DES에 적용한 차분분석 기법이 동일하게 HEA에도 적용됨을 보이고 10라운드로 축소된 HEA 경우 선택평문공격(chosen plaintext attack)이 가능하며 일정한 확률에 의해 분석됨을 증명하였다.

ABSTRACT

In this paper, we study a security of HEA(Hangul Encryption Algorithm) against differential cryptanalysis. HEA, which is 1,024bits input/output and 56bits key size, has the same structure as DES(Data Encryption Standard) only for Korean characters to be produced in ciphertexts. An encryption algorithm should be developed to meet certain critria such as input/ouput dependencies, correlation, avalanche effects, etc. However HEA uses the same S-Boxes as DES does and just expands the plaintext/ciphertext sizes.

We analysize HEA with a differential cryptanalysis and present two results. The number of rounds of HEA has not been determined in a concrete basis of cryptanalysis and we show a chosen plintext attack of 10 round reduced HEA with a differential cryptanalysis characteristic.

keyword : *DES(Data Encryption Standard),HEA(Hangul Encryption Algorithm), differential cryptanalysis*

Ⅰ. 서 론

블록 암호 알고리즘 분석 및 설계에 대한 연구는 1977년 미국연방표준으로 DES(Data Encryption Standard)가 제정되면서부터 본격적으로 진행되었다. 1980년대 까지만 해도 DES를 변형 혹은 모방한 암호 알고리즘들에 대한 안전성을 분석할 이론적 근거가 미약하였으나 DES에 대한 안전성이 수학적으로 키의 길이에 절대적으로 의존하지 않음은 1990년 E. Biham, A. Shamir의 차분분석(Differential Cryptanalysis)[2~5]과 1993년 M. Matsui의 선형근사분석 (Linear Cryptanalysis)[6]이 제안되면서 증명되었다.

블록 암호 알고리즘 설계시 알고리즘의 안전성과 효율성이 동시에 고려되여야 하며 안전성 고려사항으로 키 길이 이외에 알고리즘의 구조와 사용되는 연산들에 대해서도 고려되어야 한다. 컴퓨터 계산능력의 급속한 발달로 블록 암호 알고리즘의 안전성 기준은

* 한양대학교
** 국제과학문화연구소

과거 DES의 키 길이 56비트에서 현재 128비트 이상으로 설정되는 추세이다. 최근 미국에서는 미연방표준 DES를 대체할 표준 암호 알고리즘 AES(Advanced Encryption Standard)으로 Rijndael이 2000년 10월에 선정되었다[7]. 국내에서도 한국정보보호센터에서 개발한 128비트 SEED가 민간 표준 블록 암호 알고리즘으로 제안되고 있으며 SEED를 채택한 정보보호시스템이 속속 개발되고 있고 차세대 블록 암호알고리즘에 대한 요구도 증가하고 있다[8].

본 논문에서는 DES(Data Encryption Standard)를 변형하여 설계된 HEA 안전성에 대하여 고찰하고자 한다. 암호 알고리즘의 안전성은 크게 입출력문과 키의 크기, 평문과 암호문 및 키와 암호문의 상관성, 평문과 키의 변화에 따르는 암호문의 변화 그리고 구조적 특이성 등이 고려된다. 이러한 요구조건들을 만족시키기 위해서 비선형 함수를 포함한 세부논리를 알고리즘의 효율성을 고려하여 설계되어야 하며 그 중 대표적으로 비선형 함수를 lookup table S-box로 사용하기도 한다. 그러나 일부 암호 알고리즘들은 기존 암호 알고리즘의 세부논리를 수정없이 이용하기도 한다. 본 논문에서는 HEA의 구조와 S-box들이 DES와 동일하기 때문에 DES에 적용된 차분공격이 적용될 수 있음을 보이고 10라운드로 축소된 HEA를 차분공격법으로 분석하기로 한다.

1.1 HEA의 개요

HEA는 조합형 한글 음절들을 암호화하여 조합형 한글 음절들을 생성하는 알고리즘이다. 기존의 알고리즘으로 암호문이 출력 가능하게 되기 위해서 별도의 변환과정이 필요하지만, HEA는 평문과 암호문 모두 조합형 코드로 되어있으므로 별도로 과정을 수행할 필요가 없는 알고리즘이다.

전체적으로 DES와 동일한 구조이고 사용하는 순열도 DES와 동일하나, 입출력 블록의 크기는 64음절 (1,024비트)이다. 키 크기도 DES와 동일한 56비트이다.[9]

1.1.1 DES와 HEA에서의 연산.

HEA는 기본적으로 DES와 동일한 구조를 가지고 있으므로, DES와 비교하여서 설명한다. DES의 입력은 64비트 블록이고 HEA는 64음절 즉 1,024(64×16)비트 블록이다. 이것 외에 비트 단위를 음절 단위로 확대시킨 것 뿐 다른 구조적인 면에서는 DES와 유사하다. 입력 1,024비트에 출력도 1,024비트이고, 키는 56비트를 사용한다.

본 논문에 사용된 표기법은 다음과 같다.

(1) $R(n)$: n라운드 데이터의 오른쪽 32음절.
(2) $L(n)$: n라운드 데이터의 왼쪽 32음절.
(3) $r^n_{i,j}$: $R(n)$ i번째 음절의 초성($j=1$), 중성($j=2$), 종성($j=3$) 각 5비트.
(4) $l^n_{i,j}$: $L(n)$ i번째 음절의 초성($j=1$), 중성($j=2$), 종성($j=3$) 각 5비트.
(5) $R(n)_{XOR3D}$: n라운드에서 XOR3D 연산을 한 결과. $R(n)_{XOR3D}=XOR3D[R(n)]$.
(6) $K(n)$: n라운드에 사용되는 라운드 키.
(7) $F(n)$: n라운드 F 함수의 출력 데이터 $F(n)=F[R(n)_{XOR3D}, K(n)]$.
(8) f^n_i : n라운드 F 함수의 출력 데이터의 i번째 음소 5비트.
(9) $(***,***.....***)_{nbit}$ 혹은 $(***...***)_{nbit}$
: 각 *는 n 비트
***는 한 음절(초성,중성,종성)을 표현.

1.1.1.1 XOR3D(eXclusive-OR of 3 dimensions)

32음절을 입력받아 32개의 음소(5비트)를 생성한다. 각 음절 초성, 중성, 종성 5비트 중 같은 위치에 있는 비트별로 XOR하여 1비트를 생성, 음절 당 5비트를 생성한다.

1.1.1.2 MOD(Modular Operation)

F함수에서 나온 결과 32음소와 전 라운드의 왼쪽 32음절로 32음절을 생성한다. F함수의 결과 음소가 전 라운드 왼쪽 1음절과 대응되는데, 규칙은 초성, 중성, 종성별로 다른 MOD N을 적용한다. 초성은 $N=19$, 중성은 $N=21$, 종성은 $N=28$이다.

$$R(n+1)=L(n)\ MOD\ F(n)$$
$$=(\ldots,(l^n_{i,1}+f^n_i)_{19}(l^n_{i,2}+f^n_i)_{21}(l^n_{i,3}+f^n_i)_{28},\ldots)$$

위의 두 연산을 제외한 나머지 연산은 비트가 음절단위로 확장된 것을 제외하고는 DES의 연산과 동일하므로 생략한다.

Ⅱ. HEA 분석

2.1 HEA 차분특성

DES와 유사한 입력 차분을 만들기 위하여 6개

0	0	0	0	1	1
(00000)	(00000)	(00000)	(00000)	(00001)	(00001)
(000000)	(000000)	(000000)	(000000)	(000011)	
S1-box					
(0000)	(0000)	(0000)	(0000)	(0000)	
(00000)	(00000)	(00000)	(00000)		

〈그림 1〉 S1 Box에 대한 차분특성

의 5비트를 5개의 6비트로 변환시킨 뒤, 같은 S-box에 적용시키고, 결과인 5개의 4비트를 4개의 5비트로 재 변환시킨다. 〈그림 1〉과 같이 S-box에 대해서 만일, S-box의 입력 6 비트 차분에 대한 정보를 알고 있고, 이를 제외한 다른 입력 비트들의 차분이 모두 0이라면, 고정된 확률로 S-box의 출력 4비트 차분에 대한 정보를 알 수 있고, 이를 제외한 다른 출력 비트들의 차분은 모두 확률 1로서 0인 것을 알 수 있다. 즉, S-box에 5번 table look-up하는 것을 DES와 같이 한 번으로 축소시킬 수 있다. 그리고, 출력차분을 알 때 역으로 비트 위치를 추적하면, 고정된 확률로 입력 차분을 구할 수 있다. 이렇게 구한 차분은

$\Delta X = R(1) \oplus R(1)^* = R(1)' = (000,000,000,000,000,000,000,000,000,000,000,001,001,000,000,001,000,000,001,000,\ldots,000)_{5bit}$이다. XOR3D 연산 후 $R(1)'_{XOR3D} = (000000000001\ 10010010\ \ldots0000)_{5bit}$이 되고, 이것과 DES의 차분 $\Delta X_{DES} = (00192000) = (000000000001\ 10010010\ldots0000)_{1bit}$과의 차이는 단위가 음절과 1비트이다. 이때, ΔX에서 5비트 1(00001) 대신에 2(00010), 4(00100), 8(01000), 16(10000)을 사용하여도 무방하다.

$0 \rightarrow S1, S2 \rightarrow 0 : P=1$

$3 \rightarrow S3 \rightarrow 0 : P=\frac{8}{64}$

$50 \rightarrow S4 \rightarrow 0 : P=\frac{16}{64}$

$36 \rightarrow S5 \rightarrow 0 : P=\frac{6}{64}$

$0 \rightarrow S6 \sim S8 \rightarrow 0 : P=1$

DES와 동일한 방법으로 DC를 적용하여보자.

$$R(n) = (r^n_{1,1}\ r^n_{1,2}\ r^n_{1,3}, \ldots, r^n_{32,1}\ r^n_{32,2}\ r^n_{32,3})_{5bit}$$
$$R(n)^* = (r^{*n}_{1,1}\ r^{*n}_{1,2}\ r^{*n}_{1,3}, \ldots, r^{*n}_{32,1}\ r^{*n}_{32,2}\ r^{*n}_{32,3})_{5bit}$$
$$R(n)' = R(n) \oplus R(n)^* = (r'^n_{1,1}\ r'^n_{1,2}\ r'^n_{1,3}, \ldots, r'^n_{32,1}\ r'^n_{32,2}\ r'^n_{32,3})_{5bit}$$
$$L(n) = (l^n_{1,1}\ l^n_{1,2}\ l^n_{1,3}, \ldots, l^n_{32,1}\ l^n_{32,2}\ l^n_{32,3})_{5bit}$$
$$L(n)^* = (l^{*n}_{1,1}\ l^{*n}_{1,2}\ l^{*n}_{1,3}, \ldots, l^{*n}_{32,1}\ l^{*n}_{32,2}\ l^{*n}_{32,3})_{5bit}$$
$$L(n)' = L(n) \oplus L(n)^* = (l'^n_{1,1}\ l'^n_{1,2}\ l'^n_{1,3}, \ldots, l'^n_{32,1}\ l'^n_{32,2}\ l'^n_{32,3})_{5bit}$$

$\Delta X = R(1)' = (000,000,000,000,000,000,000,000,000,000,000,001,001,000,000,001,000,000,001,000,\ldots,000)_{5bit}$, $L(1)' = (000,000,\ldots,000,000)_{5bit}$인 차분을 택한다.

$$R(1)_{XOR3D} = (r^1_{1,1} \oplus r^1_{1,2} \oplus r^1_{1,3} \cdots r^1_{32,1} \oplus r^1_{32,2} \oplus r^1_{32,3})_{5bit}$$
$$R(1)^*_{XOR3D} = (r^{*1}_{1,1} \oplus r^{*1}_{1,2} \oplus r^{*1}_{1,3} \cdots r^{*1}_{32,1} \oplus r^{*1}_{32,2} \oplus r^{*1}_{32,3})_{5bit}$$

에서, $R(1)$과 $R(1)^*$의 차이가 종성에만 나타나도록 차분특성을 설정하였으므로

$$R(1)^*_{XOR3D} = (r^1_{1,1} \oplus r^1_{1,2} \oplus r^{*1}_{1,3} \cdots r^1_{32,1} \oplus r^1_{32,2} \oplus r^{*1}_{32,3})_{5bit}$$

이 되고,

$$R(1)'_{XOR3D} = (r^1_{1,3} \oplus r^{*1}_{1,3} \cdots r^1_{32,3} \oplus r^{*1}_{32,3})_{5bit}$$
$$= (00000000000110010010\ldots0000)_{5bit}$$

이다.

DES의 S-box 분포 표를 이용하면, HEA에서 S-box의 입력 차분이 나타나는 위치는 DES와 동일하고, F 함수 차분이 $F(1)' = (000\ldots000)_{5bit}$일 확률은 1/341이다.

$L(1)' = 0$, $F(1)' = 0$ 일 때,

$R(2)' = L(1)'$ MOD $F(1) = (000,\cdots,000)_{5bit}$ 이고, $R(2)'_{XOR3D} = (000\ldots000)_{5bit}$이므로, 확률 1로 $F(2)' = (000,\ldots,000)_{5bit}$인 결과를 얻을 수 있다.

MOD 연산시, $R(3)' = L(2)'$ MOD $F(2)'$이 $L(2)'$의 동일한 차분 특성 ΔX를 유지하여야 하는데, $F(2)' = (000\ldots000)_{5bit}$ 이지만, $L(2)'$중 0이 아닌 위치에서 $R(3)'$이 동일한 차분을 유지하지 못하는 경우가 발생한다. 예를 들어,

$L(2)' = (000,000,000,000,000,000,000,000,000,000,000,001,001,000,000,001,000,000,001,000,\ldots,000)_{5bit}$에서 차분이 0이 아닌 종성 1이 $R(3)'$에서 1,3,7,15,27,31의 값을 갖는 경우가 발생하게 된다. 구체적으로, $R(3)' = (\ldots,00\{(l^2_{1,3} + f^2_1)_{28} \oplus (l^{*2}_{1,3}$

〈표 1〉 빈도분포 표

$l^2_{i,3}\oplus l^{*2}_{i,3}$								합계
1	$(l^2_{i,3}+f^2_i)_{28}\oplus(l^{*2}_{i,3}+f^2_i)_{28}$	**1**	3	7	15	27	31	
	빈도수	**448**	224	96	64	32	32	896
2	$(l^2_{i,3}+f^2_i)_{28}\oplus(l^{*2}_{i,3}+f^2_i)_{28}$	**2**	6	14	26	30		
	빈도수	**448**	192	128	64	64		896
4	$(l^2_{i,3}+f^2_i)_{28}\oplus(l^{*2}_{i,3}+f^2_i)_{28}$	**4**	12	24	28			
	빈도수	**402**	248	122	124			896
8	$(l^2_{i,3}+f^2_i)_{28}\oplus(l^{*2}_{i,3}+f^2_i)_{28}$	**8**	20	24	28			
	빈도수	**408**	134	236	118			896
16	$(l^2_{i,3}+f^2_i)_{28}\oplus(l^{*2}_{i,3}+f^2_i)_{28}$	12	**16**	20	28			
	빈도수	134	**420**	230	112			896

$+f^2_i)_{28}\},\ldots)_{5bit}$에서, 만일 종성의 MOD 연산의 법이 32라면, $(l^2_{i,3}+f^2_i)_{32}\oplus(l^{*2}_{i,3}+f^2_i)_{32}=l^2_{i,3}\oplus l^{*2}_{i,3}$으로 차분을 계속해서 유지될 것이다. 그러나, 법이 28이므로, $l^2_{i,3}\oplus l^{*2}_{i,3}=1$일 때, $(l^2_{i,3}+f^2_i)_{28}\oplus(l^{*2}_{i,3}+f^2_i)_{28}=$ 1,3,7,15,27,31의 값들을 갖을 수 있다. 특히, 1의 차분을 유지할 확률이 1/2인 것은 〈표 1〉를 보면 알 수 있다. 이는 각 차분이 0이 아닌 음소별로 각각 적용되므로, 0이 아닌 1의 값을 갖는 음소가 12, 13,16,19번째 음절의 종성 4군데 존재하는 차분의 경우는 2^{-4}의 확률로서 차분이 유지된다. 그러므로, 전체적인 2라운드 차분의 확률은 $\frac{1}{341}\times 2^{-4}\fallingdotseq 2^{-[2.41]}$이다.

입력 차분 $l^2_{i,3}\oplus l^{*2}_{i,3}$의 값에 따른 $(l^2_{i,3}+f^2_i)_{28}\oplus(l^{*2}_{i,3}+f^2_i)_{28}$의 가능한 차분의 빈도분포는 〈표 1〉과 같다.

2.2 HEA 공격

DES의 경우와 같이 1,2,3라운드 공격법이 있다. 본 논문에서는 2,3라운드 공격법을 적용하기로 한다.

2.2.1 3라운드 공격법(<그림 2> 참조)

$$\begin{cases} R(n)=L(n-1)\ MOD\ F(R(n-1),K(n)) \\ L(n)=R(n-1) \end{cases}$$

$$\begin{cases} R(n-1)=L(n-2)\ MOD\ F(R(n-2) \\ \qquad\qquad ,K(n-1)) \\ L(n-1)=R(n-2) \end{cases}$$

$$\begin{cases} R(n-2)=L(n-3)\ MOD\ F(R(n-3) \\ \qquad\qquad ,K(n-2)) \\ L(n-2)=R(n-3) \end{cases}$$

$$\begin{aligned} R(n)&=R(n-2)\ MOD\ F(R(n-1),K(n)) \\ &=L(n-3)\ MOD\ F(R(n-3), \\ &\quad K(n-2))\ MOD\ F(L(n),K(n)) \end{aligned}$$

$$\begin{aligned} R(n)^*&=L(n-3)^*\ MOD\ F(R(n-3)^*, \\ &\quad K(n-2))\ MOD\ F(L(n)^*,K(n)) \\ &(R(n)-R(n)^*)-(L(n-3)-L(n-3)^*) \\ &=O\ MOD\ [\{F(R(n-3),K(n-2)) \\ &\quad -F(R(n-3)^*,K(n-2))\} \\ &\quad +\{F(L(n),K(n))-F(L(n)^*,K(n))\}] \end{aligned}$$

만일 $R(n-3)=R(n-3)^*$이면

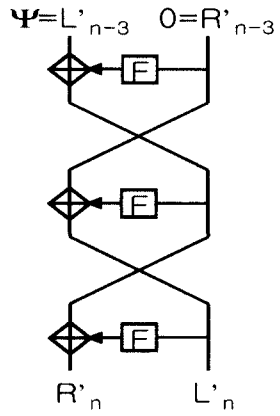
$$\begin{aligned} &(R(n)-R(n)^*)-(L(n-3)-L(n-3)^*) \\ &\quad =O\ MOD\ [F(L(n),K(n))-F(L(n)^*,K(n))] \end{aligned}$$

여기서, $(L(n-3)-L(n-3)^*)$에 대한 정보를 알기 위해, 다음과 같은 $\Psi=(L(n-3)\oplus L(n-3)^*)$을 이용하자. $\oplus$와 -을 비교하면, $\oplus$의 차분이 1이라면, -의 차분은 1 혹은 -1인 경우, 즉 차분의 절대값이 1이다. 초,중,종성의 법이 각각 다르기 때문에 그 값들을 비교하면 -의 차분이 1인지 -1인지 확인할 수 있다. 예를 들어서, $L(n-3)\oplus L(n-3)^*$ 중 $l^{(n-3)}_{i,1}\oplus l^{*(n-3)}_{i,1}=0$, $l^{(n-3)}_{i,2}\oplus l^{*(n-3)}_{i,2}=0$, $l^{(n-3)}_{i,3}\oplus l^{*(n-3)}_{i,3}=1$ 이고, $r^{(n-3)}_{i,1}\oplus r^{*(n-3)}_{i,1}=14$, $r^{(n-3)}_{i,2}\oplus r^{*(n-3)}_{i,2}=-7$, $r^{(n-3)}_{i,3}\oplus r^{*(n-3)}_{i,3}=15$라면, $f^n_i-f^{*n}_i=14$임을 확인할 수 있고, 추가적으로, $l^{(n-3)}_{i,3}-l^{*(n-3)}_{i,3}=1$이다. $f^n_i-f^{*n}_i$는 초,중,종성에 각각 적용되므로, 두 음소만 알고 있어도 나머지 한 음소의 차이를 알 수 있다.

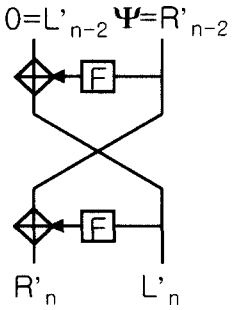
2.2.2 2라운드 공격법(<그림 3> 참조)

$$\begin{cases} R(n)=L(n-1)\ MOD\ F(R(n-1),K(n)) \\ L(n)=R(n-1) \end{cases}$$

$$\begin{cases} R(n-1)=L(n-2)\ MOD\ F(R(n-2) \\ \qquad\qquad ,K(n-1)) \\ L(n-1)=R(n-2) \end{cases}$$



〈그림 2〉 3라운드 공격



〈그림 3〉 2라운드 공격

$$R(n) = R(n-2)\ MOD\ F(L(n), K(n))$$
$$R(n)^* = R(n-2)^*\ MOD\ F(L(n)^*, K(n))$$
$$(R(n) - R(n)^*) - (R(n-2) - R(n-2)^*)$$
$$= O\ MOD[F(L(n), K(n)) - F(L(n)^*, K(n))]$$

만일 $R(n-2) = R(n-2)^*$라면,

$$R(n) - R(n)^*$$
$$= O\ MOD[F(L(n), K(n)) - F(L(n)^*, K(n))]$$

나머지는 3라운드 공격법과 동일하게 적용된다.

Ⅲ. 결 론

본 논문에서는 DES를 변형하여 설계된 HEA에 대하여 고찰하였다. 반복구조를 갖는 블록암호알고리즘 설계시 자체분석을 통하여 어느정도의 안전성 여유분(safety margin)을 고려하여 라운드 수를 설정하지만 HEA에서는 그에 대한 설명이 없다[9,10]. 비록 10라운드로 축소된 HEA를 차분특성을 이용하여 분석하였으나 설계당시 제시하지 못하였던 차분특성을 발견하였다. 한글로 입출력이 가능하도록 DES를 변형하여 설계된 HEA의 안전성은 키의 길이가 DES와 동일한 56비트이므로 키 전수조사공격 복잡도로는 그 안전성을 논할 수 없다. 또한, 차분특성을 찾기 어렵게 하기 위해 배타적 논리합 대신 모듈러 연산을 사용하였으나, 본 논문에서 소개된 바와 같이 차분특성을 찾았다.

HEA의 차분특성은 DES와 다르게 확률의 증가없이 1라운드를 추가할 수 없다. HEA 차분특성을 이용하면, 2라운드 반복 차분특성을 3번 반복함으로 6라운드의 차분특성을 만들고, $\frac{8}{64} \times \frac{16}{64} \times \frac{6}{64} = 2^{-8.41}$의 확률로 1라운드를 추가한 후 3라운드 공격을 하면, 10라운드 선택평문공격이 가능하고, $(2^{-12.41})^3 \times 2^{-8.41} = 2^{-45.64}$의 확률로 HEA가 분석된다.

향후 연구과제로는 HEA의 안전성 및 효율성을 확보할 수 있는 S-Box구성방안, 라운드 수 결정 등을 이론적으로 증명하는 것이다.

참 고 문 헌

[1] Bruce Schneier, Applied Cryptography - Protocols, Algorithms, and Source Cdoe in C, John Wiley & Sons, Inc., 1994.

[2] Eli Biham, Adi Shamir, "Differential Cryptanalysis of DES-like cryptosystems," Advances in Cryptology-Proceedings of CRYPTO'90, Lecture Notes in Computer Science 537, Springer-Verlag, 1991, pp. 2~21.

[3] Eli Biham, Adi Shamir, "Differential Cryptanalysis of DES-like cryptosystems," Journal of Cryptology, VOL. 4, No. 1, Springer-Verlag, 1991, pp. 3~72.

[4] Eli Biham, Adi Shamir, "Differential Cryptanalysis of the Full 16-round DES," Advance in Cryptology-CRYPTO'92, Springer-Verlag Lecture Notes in Computer Science 740, 1993, pp. 487~496.

[5] K.Nyberg and L.R.Knudsen, "Provable security against differential crypanalysis," Avances in Cryptology-Proceedings of CRYPTO'92, Lecture Notes in Computer Science, Vol. 740, Springer-Velag, 1993, pp. 566~574

[6] M.Matsui, "Linear Cryptanalysis method for DES cipher," Advance in Cryptology-EURCRYPT'93, ed. T.Helleseth, Volume 765 of Lecture Notes in Computer Science, Springer-Verlag, Berlin, Heidelberg, New York, 1994, pp. 386~397.

[7] James Nechvatal, Elaine Barker, Lawrence Bassham, William Burr, Morris Dworkin, James Foti, Edward Roback," Report on the Development of the Advanced Encryption Standard(AES)," NIST public document, http://csrc.nist.gov/encryption/aes, 2000.

[8] 한국정보보호센터, "128비트 블록 암호 알고리즘(SEED)개발 및 분석보고서", http:\\www.kisa.or.kr/technology/sub1/128-seed.pdf

[9] 김윤정, 박근수, 조유근, "DES에 기반한 조합형 한글 암호 알고리즘", 한국통신정보보호학회, 통신정보보호학회논문지, 제9권, 제3호, 1999.

[10] 김윤정, 박근수, 조유근, "DES에 기반한 한글-영문 암호 알고리즘", 한국통신정보보호학회, 통신정보보호학회 종합학술발표회 논문집 Vol 9, No.1, 1999.

[11] Masayuki Kanda,Youichi Takashima, Tsutomu Matsumoto, Kazumaro Aoki, and Kazuo Ohta, "A Strategy for constructing fast round functions with practical security against differential and linear cryptanalysis," 5th Annual International Workshop, SAC'98, Vol. 1556, Lecture Notes in Computer Science, Springer-Verlag, 1998, pp. 264~279.

[12] 송정환, 조용국, 현진수, 강형석, "DES변형 블록암호알고리즘 HEA에 대한 분석", 제12회 정보보호와 암호에 관한 학술대회(WISC2000) 논문집, 2000, pp. 309~320.

[13] 성수학, 박상우, 강주성, 지성택, "SPN구조에서 최적의 선형변환을 찾는 알고리즘," 제12회 정보보호와 암호에 관한 학술대회(WISC2000) 논문집, 2000, pp. 189~197.

〈著者紹介〉

현 진 수 (Jin Su Hyun) 학생회원
2000년 2월 : 한양대학교 수학과 이학사
2000년 3월~현재 : 한양대학교 수학과 석사과정
〈관심분야〉 암호학

송 정 환 (Jung Hwan Song) 정회원
1984년 2월 : 한양대학교 수학과 이학사
1989년 5월 : Syracuse University, Mathematics 석사
1993년 5월 : Rensselaer Polytechnic Institute, Mathematics 박사
1999년 3월~현재 : 한양대학교 수학과 조교수
〈관심분야〉 수리계획법,암호학

강 형 석 (Hyung Suk Kang) 정회원
1981년 2월 : 한양대학교 수학과 이학사
1988년 6월 : 한양대학교 전자계산학과 석사
1996년 3월 : 요코하마국립대학교 공학박사
현재 : 국제과학문화연구소 책임연구원
〈관심분야〉 암호정책, 접근제어, 암호학