情報保護學會論文誌
第13券 第1號, 2003. 2

CIKS-1 블록 암호에 대한 선택 평문 선형 공격

이 창 훈*, 홍 득 조*, 이 성 재**, 이 상 진*, 양 형 진*, 임 종 인*

A Chosen Plaintext Linear Attack On Block Cipher Cipher CIKS-1

Chang-hoon Lee*, Deuk-jo Hong*, Sung-jae Lee**, Sang-jin Lee*,
Hyung-jin Yang*, Jong-in Lim*

요 약

본 논문에서는 선형 공격으로 5라운드로 줄인 블록 암호 CIKS-1에 대한 안전성을 평가하고, 이 공격을 전체 라운드(8라운드)까지 정규적으로 확장할 수 있음을 보인다. CIKS-1은 크게 데이타 의존 치환들과 내부 키 스케줄링으로 구성된다. 우리는 CIKS-1 암호의 구조적인 특성을 고려하여 선형 근사식을 찾는다. 즉, 한 라운드 선형 근사식을 만들기 위해 병렬 처리가 가능한 16개의 2비트 덧셈 연산("+...+")에 대해 확률(p)이 3/4인 16개의 선형 근사식을 고려하고, Piling-Up 정리를 이용하여 확률(P)이 $1/2+2^{-17}$인 한 라운드 선형 근사식을 추출한다. 그리고 난 후, 이 한 라운드 근사식을 이용하여 확률이 $1/2+2^{-17}$인 3라운드 선형 근사식을 찾아서 5라운드 CIKS-1를 공격한다. 또한 동일한 3라운드 근사식을 이용하여 공격을 8라운드 CIKS-1로 확장한다. 결과로서 우리는 99.9% 성공 확률로 5라운드 CIKS-1 암호의 마지막 라운드 키를 찾는데 약 2^{38}개의 선택 평문과 $2^{67.7}$정도의 암호화 시간이 필요함을 제안한다.(또한, 8라운드 CIKS-1의 경우에도 2^{38}개의 선택 평문을 가지고 99.9% 성공 확률로 마지막 라운드 키를 찾을 수 있다. 다만, 약 2^{166} 암호화 시간이 요구된다.)

ABSTRACT

In this paper, we firstly evaluate the resistance of the reduced 5-round version of the block cipher CIKS-1 against linear cryptanalysis(LC) and show that we can attack full-round CIKS-1 with 256-bit key through the canonical extension of our attack. A feature of the CIKS-1 is the use of both Data-Dependent permutations(DDP) and internal key scheduling which consist in data dependent transformation of the round subkeys. Taking into accout the structure of CIKS-1 we investigate linear approximation. That is, we consider 16 linear approximations with p=3/4 for 16 parallel modulo 2^2 additions to construct one-round linear approximation and derive one-round linear approximation with the probability $P=1/2+2^{-17}$ by Piling-up lemma. Then we present 3-round linear approximation with $1/2+2^{-17}$ using this one-round approximation and attack the reduced 5-round CIKS-1 with 64-bit block by LC. In conclusion we present that our attack requires 2^{38} chosen plaintexts with a probability of success of 99.9% and about $2^{67.7}$ encryption times to recover the last round key.(But, for the full-round CIKS-1, our attack requires about 2^{166} encryption times)

Keyword : *Block cipher, A cipher with internal key schedule, Linear Cryptanalysis, A chosen plaintext attack, Data-dependent permutation*

Ⅰ. 서 론

데이터 의존 연산들(Data-Dependent Operation)은 암호학적으로 흥미로운 것이다. 그 중에 데이터 의존 순환(Data-Dependent Rotation(DDR)) 연산은 가장 잘 알려진 것으로, Rivest가 제안한 RC5[12]와 최근 AES

* 고려대학교 정보보호기술연구센터(CIST)({crytpo77, hongdj, sangjin, jilim}@cist.korea.ac.kr, yangh@korea.ac.kr)
** 한국정보보호진흥원(KISA)(sjlee@kisa.or.kr)

후보 알고리즘으로 제안된 RC6[10]와 MARS[2] 암호는 이 연산을 사용한다. 그리고 이러한 DDR 연산은 다른 간단한 연산들을 함께 혼합하여 사용할 경우 선형 분석을 효율적으로 막을 수 있다는 사실이 제시되기도 하였다.[11] 그러나 최근 FSE02에서 T. Shimoyama는 다중 선형 공격으로 취약 키를 가지고 있는 18라운드 RC6를 공격할 수 있음을 보였고,[13] ICICS2002에서 A. Miyaji는 $2^{123.9}$개의 평문을 가지고 성공 확률 90%로 17라운드 RC6를 공격할 수 있는 효율적인 알고리즘을 제안하였다.[14]

본 논문에서는 Journal of Cryptology(Vol.15 Num.1 winter 2002)[8]에서 소개한 블록 암호 CIKS-1를 소개하고 선형 공격으로 5라운드로 줄인 CIKS-1 암호에 대한 안전성을 분석하고 이 공격을 전체 라운드 CIKS-1까지 정규적으로 확장할 수 있음을 보인다.

먼저 우리는 CIKS-1 암호의 구조적인 특성을 고려하여 선형 근사식을 찾는다. 즉, 한 라운드 선형 근사식을 만들기 위해 16개의 2비트 덧셈 연산("+...+")에 대한 확률(p)이 3/4인 16개의 선형 근사식을 고려한다. 그리고 Piling-Up 정리를 이용하여 확률(P)이 $1/2+2^{-17}$인 한 라운드 선형 근사식을 추출한다. 그런 다음, 이 한 라운드 근사식을 이용하여 확률이 $1/2+2^{-17}$인 3라운드 선형 근사식을 꾸며서 160비트 키를 사용하는 5라운드 CIKS-1를 공격한다. 또한 이 특성은 256비트 키를 사용하는 8라운드 CIKS-1에 대한 공격 확장에도 사용될 수 있다. 여기서 우리는 5라운드 CIKS-1에 대한 공격 방법을 중점적으로 언급하고 8라운드 CIKS-1의 공격에 대한 적용 방법을 간략히 소개한다.

그리고 결과로서 99.9%의 성공 확률로 5라운드 CIKS-1암호의 마지막 라운드 키를 찾는데 약 2^{38}개의 선택 평문과 $2^{67.7}$ 정도의 암호화 시간이 요구됨을 제안한다.(또한 8라운드 CIKS-1 암호의 경우에도 5라운드 CISK-1 공격과 동일한 성공확률과 선택 평문수로 키를 찾을 수 있음을 제시한다. 다만 약 2^{166}정도의 암호화 시간이 요구된다.)

II. CIKS-1 알고리즘 소개

CIKS-1(a Cipher with Internal Key Scheduling)은 A. A. Moldovyan과 N. A. Moldovyan에 의해 소개된 알고리즘으로서[8] 크게 데이타 의존 치환들과 내부 키 스케줄링으로 구성된다. 이번 장에서는 CIKS-1에 사용되는 치환인 CP-박스들(CP-boxes)의 특성을 알아보고 CIKS-1이 수행되는 과정을 설명한다. 앞으로 우리는 [8]에서 사용되는 정의와 표기법들을 그대로 사용할 것이다.

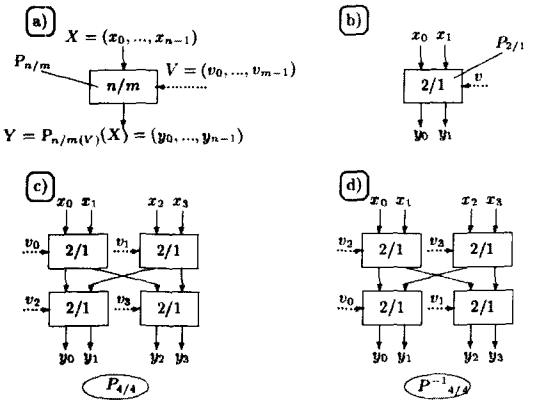
2.1 기본 성질

[정의 1]

입력 벡터 $X=(x_0,\cdots,x_{n-1})$와 제어 벡터(controlling vector) $V=(v_0,\cdots,v_{m-1})$를 피연산자라고 하고 출력 벡터를 $Y=(y_0,\cdots,y_{n-1})$라 하자. 그리고, 순서 집합 $\Pi_V=\{\Pi_0,\Pi_1,\cdots,\Pi_{2^m-1}\}$를 어떤 n비트 집합들이 임의 V에 의해 제어된 치환들의 집합(or CP-modification)이라 하자. 그러면 CP연산 $P_{n/m}(X)$는 다음과 같이 정의 될 수 있다.

$$Y=P_{n/m}(X)=\Pi_V(X)$$

CP-박스들의 모습은 [그림 1]과 같다. 그리고 일반적으로 제어 벡터 V는 암호화 된 데이터와(또는) 키에 의존한다고 가정하고 CP-박스들은 기본이 되는 치환 $P_{2/1}$-박스를 겹쳐 사용함으로써 만들 수 있다. $P_{2/1}$-박스는 한 비트 제어 벡터 v에 의해 제어되는데, 만약 $v=0$이면 $P_{2/1}$-박스의 입력 두 비트는 서로 위치가 바뀌어 출력되고 그렇지 않으면($v=1$) 입력 두 비트는 바뀌지 않고 그대로 출력된다.



〔그림 1〕 기본 CP-박스 치환들의 구조

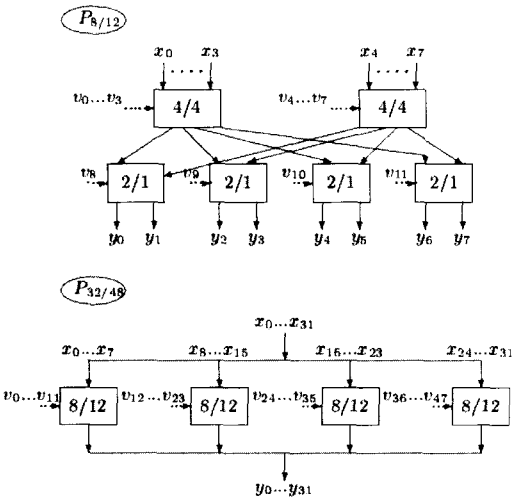
[정의 2]

1. $P_{n/m}$-박스에 대해 n비트보다 작은 임의 h비트 입력 벡터를 $x_0,\cdots,x_h$ 임의 h비트 출력 벡터를 $y_0,\cdots,y_h$라 가정하자. 그러면 모든 $i=1,2,\cdots,h$에 대해 x_i에서 y_i로 움직이는 CP-modification이 적어도 하나

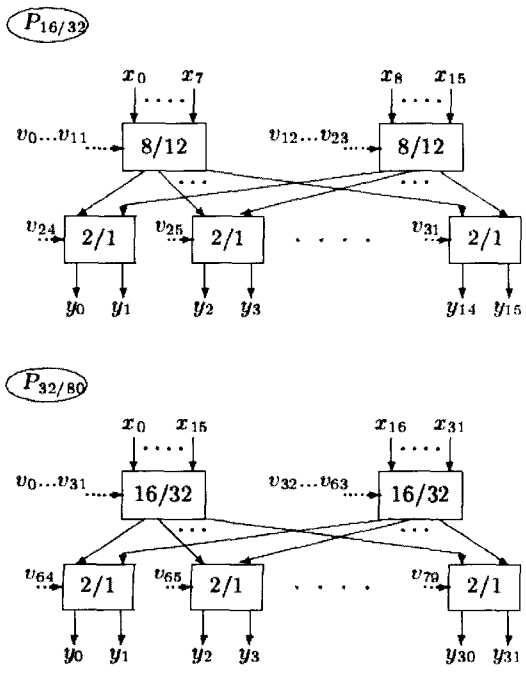
존재한다.

2. 만약 가능한 V벡터의 모든 값에 대해 대응하는 CP-modification Π_V와 $\Pi_V{}^{-1}$가 서로 역관계를 가지면 CP-박스 $P_{n/m}$와 $P_{n/m}{}^{-1}$는 서로 역관계에 있다.

[그림 2]와 [그림 3]은 CP-박스들의 변이들로서 블록 암호 CIKS-1의 구성 요소들이다.



〔그림 2〕 CP-박스 치환들



〔그림 3〕 CP-박스 치환들

2.2 블록 암호 CIKS-1

블록 암호 CIKS-1의 설계원리는 CP-박스 치환들을 사용하여 빠르고 저렴한 비용으로 하드웨어 구현을 쉽게 할 수 있도록 하는 것에 기초를 두고 있다. CIKS-1는 64비트 블록과 256비트 비밀키를 사용하여 8라운드를 반복하는 블록 암호이다. 마스터 키 K는 8개의 32비트로 나뉘고 각 32비트는 차례대로 각 라운드 함수의 부분 키로서 사용된다(즉, $K = K^1 \| \cdots \| K^8$). 그런데, 각 라운드 함수에는 32비트 부분 키들을 변환하는 내부 키 생성과정이 포함되어 있어서 사실상 비밀키의 부분 32비트와 실제로 라운드 암호화에 쓰이는 라운드 부분키는 다르다고 말할 수 있다.

CIKS-1의 한 라운드 구조는 [그림 4]와 같다. 한 라운드에는 CP-박스 치환들과 함께 고정된 치환들(Π_1, Π_2, 7비트 순환 연산), XOR(exclusive-or)연산과 병렬 연산이 가능한 16개의 2비트 덧셈(뺄셈)이 사용된다. 위의 덧셈(뺄셈) 연산을 "+...+"("-...-")로 쓴다.

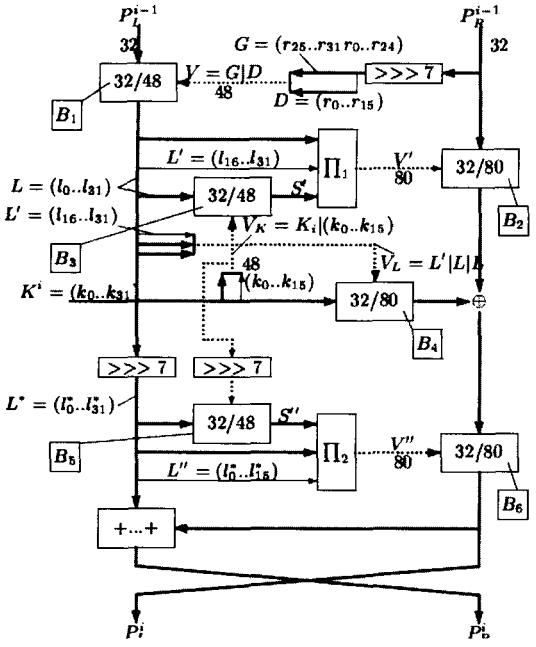
<연산>

1. 병렬 연산이 가능한 16개의 2비트 덧셈 연산("+...+" modulo 2^2additions)은 하나의 32비트 덧셈 연산(modulo 2^{32} addition)을 대신해서 왼쪽 블록과 오른쪽 블록을 입력으로 하여 암호화 과정을 수행한다. 즉, 왼쪽 블록과 오른쪽 블록의 각 32비트 피연산자들을 16개의 2비트로 나누어서 병렬로 동시에 2비트를 덧셈 연산을 수행한다.
2. 치환 Π_1와 Π_2는 다음을 따른다.

$$\begin{aligned} V' &= (v'_0, \cdots, v'_{79}) = \Pi_1(L \mid L' \mid S') \\ &= \Pi_1(l_0, \cdots, l_{31}, l_{16}, \cdots, l_{31}, s'_0, \cdots, s'_{31}) \\ &= (l_8, \cdots, l_{31}, s'_0, \cdots, s'_7, l_{16}, \cdots, l_{31}, l_0, \cdots, l_7, \\ &\quad s'_8, \cdots, s'_{31}) \end{aligned}$$

$$\begin{aligned} V'' &= (v''_0, \cdots, v''_{79}) = \Pi_2(S'' \mid L^* \mid L'') \\ &= \Pi_2(s''_0, \cdots, s''_{31}, l^*_0, \cdots, l^*_{31}, l^*_0, \cdots, l^*_{15}) \\ &= (s''_{16}, \cdots, s''_{23}, l^*_0, \cdots, l^*_3, s''_{24}, \cdots, s''_{31}, l^*_4, \\ &\quad \cdots, l^*_{15}, s''_0, \cdots, s''_7, l^*_{16}, \cdots, l^*_{19}, s''_8, \cdots, \\ &\quad s''_{15}, l^*_{20}, \cdots, l^*_{31}, l^*_0, \cdots, l^*_{15}) \end{aligned}$$

위의 연산들이 수행되는 과정은 CIKS-1의 한 라운드 암호화 과정([그림4])을 보면 쉽게 이해 할 수 있다.



〔그림 4〕 CIKS-1의 i번째 라운드 변환

Ⅲ. CIKS-1에 대한 선형 분석

이 절에서는 CIKS-1에 대한 선형 분석을 소개한다. 선형 분석(Linear Cryptanalysis, LC)은 블록 암호에 대한 공격법 중에서 차분 공격(Differential Cryptanalysis, DC)과 더불어 가장 강력한 공격 방법이다.[6] Matsui가 소개한 이 공격 방법은 평문과 암호문 그리고 부분키 정보와의 선형 관계를 조사하여 분석하는 기지 평문 공격이다. 즉, 주어진 평문과 대응하는 암호문에 대해 반복되는 암호의 각 라운드의 근사식을 결합하여 선형 근사식의 확률이 $p \neq 1/2$인 다음과 같은 선형 근사식을 찾아 Matsui[6]가 제안한 알고리즘 2를 적용하여 키 비트를 찾는다.

$$P[i_1, i_2, \cdots, i_a] \oplus C[j_1, j_2, \cdots, j_b] = K[k_1, k_2, \cdots, k_c]$$

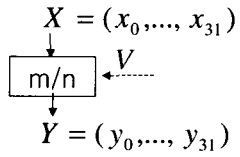
여기서, $P[i_1, i_2, \cdots, i_a] = P[i_1] \oplus, \cdots, \oplus P[i_a]$을 의미하고, $i_1, \cdots, i_a$ 는 고정된 비트 위치를 말한다.

3.1 선형 공격을 위한 접근 방법

CIKS-1 암호에 대한 선형 공격의 안전성을 평가하기 위해 필요한 CIKS-1 암호의 특성 및 선형 근사식을 만드는 방법에 대해 논한다.

<접근 방법>

1. CP-박스들(치환들)의 입력 X의 모든 비트들의 합 $X[x_0, \cdots, x_{31}]$을 $X[all]$라 하고, 출력 Y의 모든 비트들의 합을 $Y[all]$라 하면, 제어 벡터 V에 상관 없이 항상 $X[all] = Y[all]$가 성립한다. 왜냐하면 CP-박스들은 치환들이기 때문에 Y는 단지 X의 재배열에 불과하다.



〔그림 5〕 CP-박스 특성

2. 한 라운드 선형 근사식을 만들기 위해 병렬 연산이 가능한 16개의 2비트 덧셈 연산들("+CDOTS +")을 고려한다. 그리고 "+ ⋯+"에 대한 피연산자를 $L = (l_0, \cdots, l_{31})$과 $R = (r_0, \cdots, r_{31})$이라고 하고 "+ ⋯+"에 대한 출력 값을 $M = (m_0, \cdots, m_{31})$라 하자. 그러면 다음과 같은 16개의 근사식을 세울 수 있다.

$$\begin{aligned}
&l_0 l_1 + r_0 r_1 = l_0 l_1 \oplus r_0 r_1 \\
&l_2 l_3 + r_2 r_3 = l_2 l_3 \oplus r_2 r_3 \\
&\cdots\cdots\cdots\cdots \\
&l_{30} l_{31} + r_{30} r_{31} = l_{30} l_{31} \oplus r_{30} r_{31} \\
&\qquad\qquad \Leftrightarrow \\
&l_0 \oplus l_1 \oplus r_0 \oplus r_1 = m_0 \oplus m_1 \\
&l_2 \oplus l_3 \oplus r_2 \oplus r_3 = m_2 \oplus m_3 \\
&\cdots\cdots\cdots\cdots \\
&l_{30} \oplus l_{31} \oplus r_{30} \oplus r_{31} = m_{30} \oplus m_{31}
\end{aligned}$$

이 16개의 모든 근사식들은 확률 $p = 3/4$로서 성립함을 쉽게 확인 할 수 있고, Piling-Up 정리를 이용하여 아래와 같은 확률이 $P = 1/2 + 2^{-17}$인 CIKS-1의 한 라운드 선형 근사식을 찾을 수 있다.

$$L[l_0, \cdots, l_{31}] \oplus R[r_0, \cdots, r_{31}] = M[m_0, \cdots, m_{31}]$$

3. 만약 첫 번째 라운드의 $L^1 = (l_0, \cdots, l_{31})$을 다음 집합 A와 같은 형태를 가지도록 하는 평문 (P_L^1, P_R^1)을 선택한다면 CIKS-1의 첫째 라운드의 선형 근사식 확률은 $P = 1$를 따른다. 왜냐 하면 이 경우

에 "+…+"에 대한 16개의 선형 근사식들에 대한 확률이 각각 모두 1을 만족하기 때문이다.

$$A=[L^1(l_0,\cdots,l_{31})|\text{모든 } i\text{에 대해 } (0\le i\le 15),\ l_{2i+1}=0]$$
$$=[(l_0,0,0,\cdots,0),(l_0,0,l_2,0,\cdots,0),\cdots,$$
$$(l_0,0,l_2,0,\cdots,l_{30},0),(0,0,l_2,0,\cdots,0),\cdots,$$
$$(0,0,l_2,0,\cdots,l_{30},0),\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots,$$
$$(0,\cdots.,0,l_{30},0)]$$

이러한 성질을 만족하는 평문들은 쉽게 선택할 수 있다. 왜냐하면, $L^1=(l_0,\cdots,l_{31})$은 키 요소와 상관이 없기 때문에 A집합과 같은 L^1을 선택할 수 있다. 그러면 7비트 왼쪽 순환을 통해 B_1^1박스의 출력 벡터들을 구할 수 있고, 또한 임의로 32비트 평문 오른쪽 데이터 P_R^1를 선택하여 B_1^1 제어 벡터를 만들 수 있다. 따라서, 두 벡터(B_1^1의 출력 벡터와 제어 벡터)를 가지고 B_1^1박스를 복호화하면 원하는 형태의 평문을 얻을 수 있다. 그리고 이런 평문은 2^{48}개 정도 생성할 수 있다(A의 원소 개수×가능한 $P_R^1(B_1^1)$의 수 $2^{16}\times 2^{32}=2^{48}$).

3.2 5라운드 CIKS-1 암호에 대한 선택 평문 공격

이 절에서는 우리 공격에 이용하는 3라운드 선형 근사식을 소개하고 이 특성을 사용하여 160비트 비밀키를 가지는 5라운드 CIKS-1 암호에 대한 선형 공격을 한다. 그런데, 만약 누군가가 256비트 비밀키를 사용하는(8라운드인) CIKS-1를 사용하기를 고집한다면 우리는 5라운드 공격을 정규 확장하여 그것 역시 공격 할 수 있다. 이것은 비밀키를 나누어 그대로 라운키 입력으로서 사용하는 라운드 키 생성 과정의 취약점에 기인한다. 여기서는 5라운드 줄인 CIKS-1에 대한 선형 공격만을 중점적으로 논할 것이고 8라운드 CIKS-1에 대한 공격은 간략히 소개할 것이다. [그림 6]은 우리 공격 모델을 나타내고 있다.

$P_L^i(P_R^i)$를 CIKS-1 암호의 i번째 라운드의 왼쪽(오른쪽) 입력이라고 하고 i번째 라운드의 선형 특성 확률(linear characteristic probability)을 $LCP_i=|2P_i-1|^2$라고 정의하자. 여기서 P_i는 i번째 라운드의 선형 근사식 확률을 의미한다. 먼저 공격을 하기 위한 첫 과정으로 앞절 접근 방법 3에서 제시한 평문들을 선택한다. 그러면 접근 방법 1,2를 이용하여 5라운드 CIKS-1 암호에 대해 최대 확률을 가지는 3라운드 선형 근사식을 추출할 수 있다. 이 선형 근사식은 [그림 6]에서 보여주고 있고 이 선형 근사식을 생성하는 과정은 다음과 같다.

첫번째 라운드에서 다음을 관찰 할 수 있다.

$$P^1{}_L[all]=B^1{}_1[all]=L^1[all],$$
$$P^1{}_R[all]=B^1{}_2[all]$$
$$\Rightarrow B^1{}_6[all]=K^1[all]\oplus P^1{}_R[all]=R^1[all]$$

여기서 B_j^i는 i번째 라운드의 B_j박스의 임의의 입력(또는 출력) 벡터를 의미한다. 그러면, 확률 $P_1=1$로 $L^1[all]\oplus R^1[all]=M^1[all]$가 성립함을 알 수 있고 첫 번째 라운드의 선형 근사식은 다음과 같이 간단히 정리 할 수 있다([그림 6].

$$P^1{}_R[all]\oplus P^2{}_L[all]=K^1[all]\ ;P_1=1$$
$$P^1{}_L[all]\oplus P^1{}_R[all]\oplus P^2{}_R[all]=K^1[all];P_1=1$$

또한, 두 번째 라운드에서 다음 관계를 관찰할 수 있다.

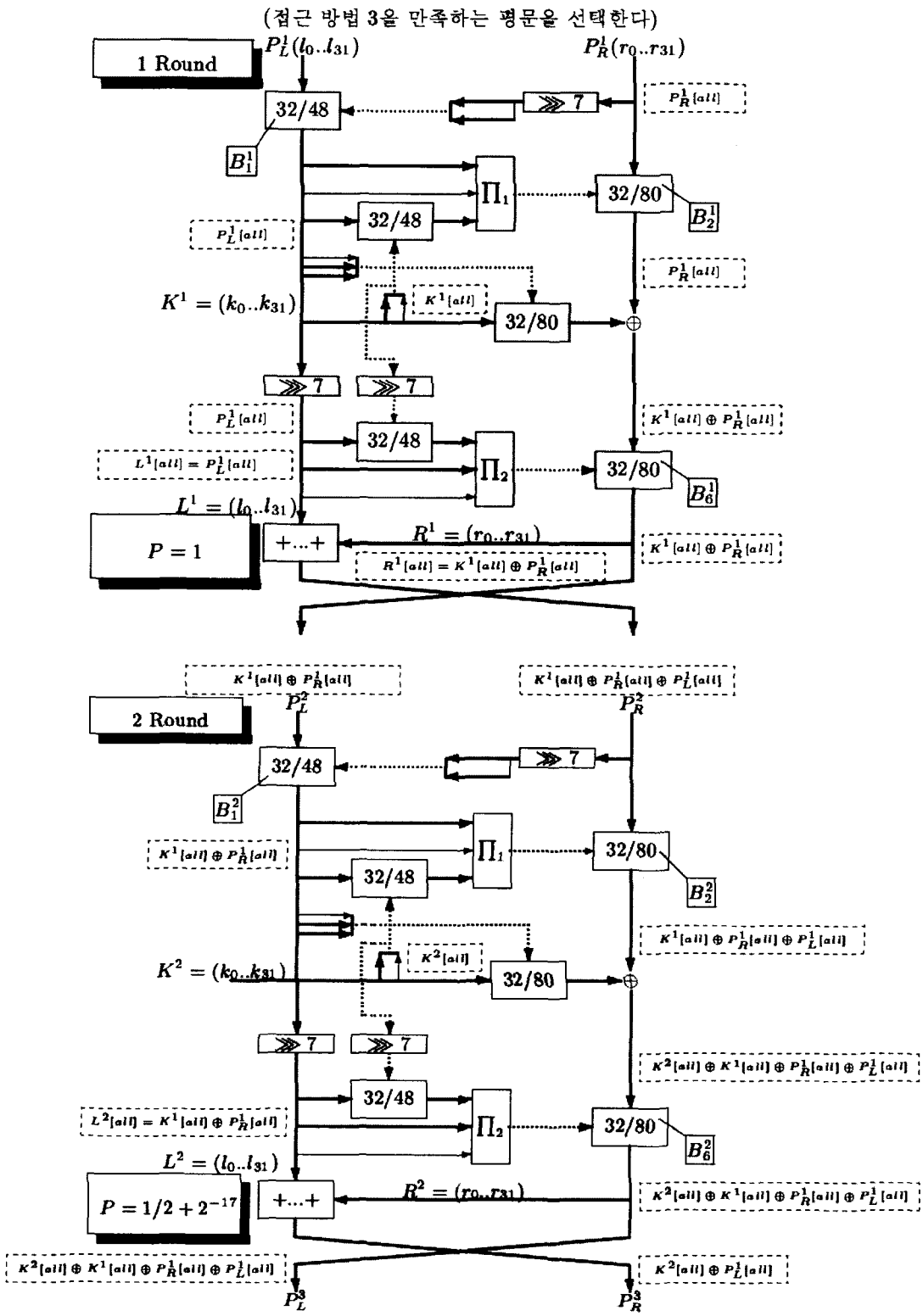
$$P^2{}_L[all]=K^1[all]\oplus P^1{}_R[all]=B^2{}_1[all]=L^2[all]$$
$$P^2{}_R[all]=K^1[all]\oplus P^1{}_L[all]\oplus P^1{}_R[all]=B^2{}_2[all]$$
$$\Rightarrow B^2{}_6[all]=K^2[all]\oplus B^2{}_2[all]=R^2[all]$$

그러면, 아래 식이 확률 $P_2=1/2+2^{-17}$로 성립함을 알 수 있다.

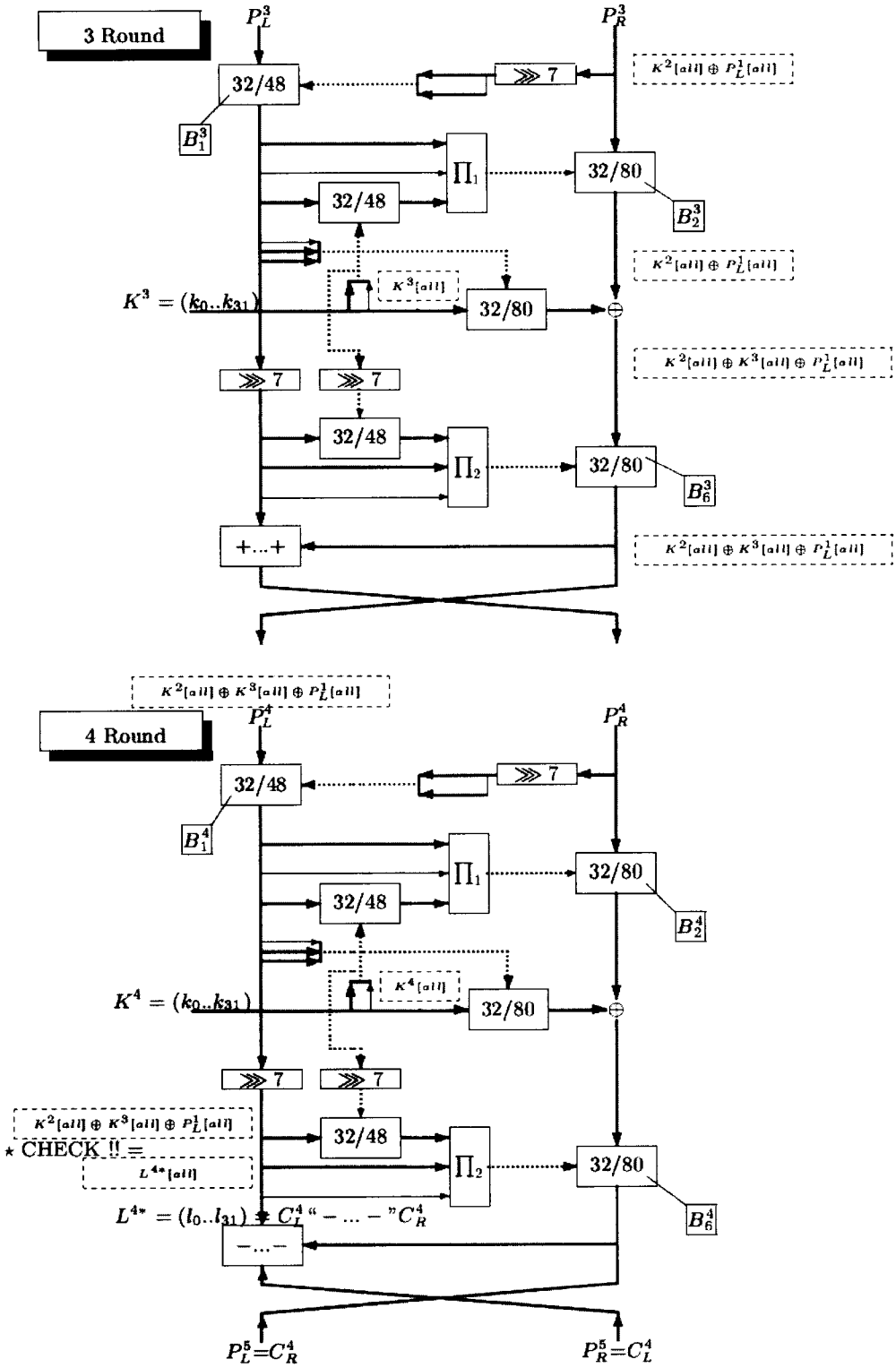
$$L^2[all]\oplus R^2[all]=M^2[all]$$
$$\Leftrightarrow\ (K^1[all]\oplus P^1{}_R[all])\oplus$$
$$(K^1[all]\oplus K^2[all]\oplus P^1{}_R[all]\oplus P^1{}_L[all])$$
$$=P^1{}_L[all]\oplus K^2[all]=M^2[all]$$

따라서, 두 번째 라운드의 선형 근사식을 정리하면 다음과 같다([그림 6]).

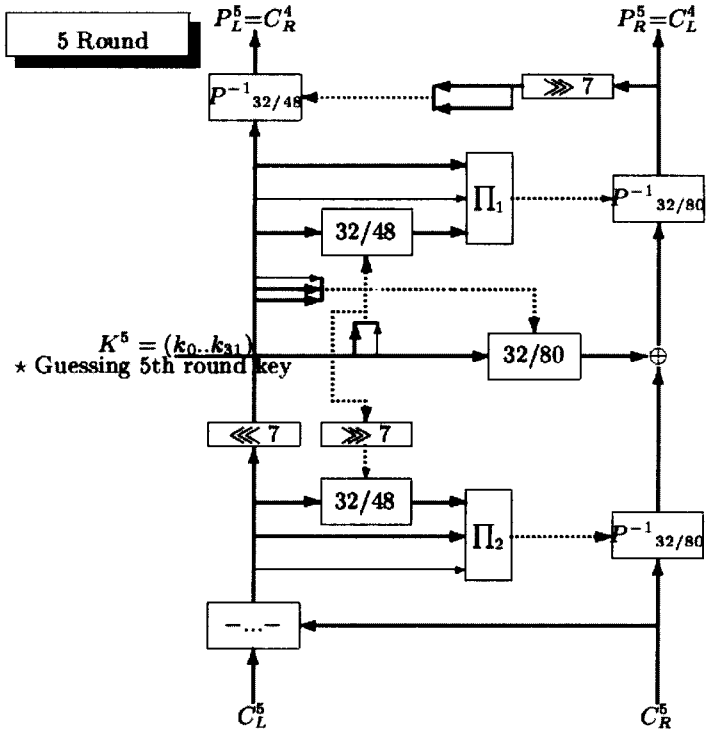
$$P_R^2[all]\oplus P_L^3[all]=K^2[all]\ ;P_2=1$$
$$P_L^2[all]\oplus P_L^3[all]\oplus P_R^3[all]=0\ ;$$
$$P_2=1/2+2^{-17}\ \text{이고}\ \ LCP_2=4\times 2^{(-17)^2}=2^{-32}$$



〔그림 6〕 CIKS-1에 대한 공격 모델(계속)



〔그림 6〕 CIKS-1에 대한 공격 모델(계속)



〔그림 6〕 CIKS-1에 대한 공격 모델

세 번째 라운드에서도 다음과 같은 관계를 찾을 수 있다. 이 라운드에서는 "+,⋯,+"에 대한 근사식은 고려하지 않는다. 다만 확률 1을 따르는 다음 식을 이용한다.

$$P^3{}_R[all] = P^1{}_L[all] \oplus K^2[all] = B^3{}_2[all]$$
$$\Rightarrow B^3{}_6[all] = K^3[all] \oplus K^2[all] \oplus P^1{}_L[all]$$
$$= R^3[all]$$

그러면, 세 번째 라운드의 선형 근사식을 다음과 같이 만들 수 있다([그림 6]).

$$P_R^3[all] \oplus P_L^4[all] = K^3[all] \ : \ P_{3'} = 1$$

따라서, 우리는 이러한 한 라운드 선형 근사식들을 모두 XOR하면 다음과 같은 5라운드 CIKS-1에 대한 연속하는 3라운드에 대한 근사식을 이끌어 낼 수 있다.

$$(P_R^1[all] \oplus P_L^2[all] = K^1[all])$$
$$\oplus (P_L^1[all] \oplus P_R^1[all] \oplus P_R^2[all] = K^1[all])$$
$$\oplus (P_R^2[all] \oplus P_L^2[all] = K^2[all])$$
$$\oplus (P_L^2[all] \oplus P_L^3[all] \oplus P_R^3[all] = 0)$$
$$\oplus (P_R^3[all] \oplus P_L^4[all] = K^3[all])$$
$$\Rightarrow P_L^4[all] = K^2[all] \oplus K^3[all] \oplus P_L^1[all]$$

Piling-Up 정리에 의해 이 3라운드 선형 근사식 확률은 $P = 1/2 + 2^{-17}$이며 $LCP = LCP_2 = 2^{-32}$이다.

본 고에서는 이 선형 근사식을 이용하여 5라운드 CIKS-1 암호를 공격한다. 먼저 선택한 평문에 대해 대응하는 암호문을 얻는다. 그런 다음 다섯 번째 라운드 키를 추측하여 라운드를 복호화하여 C_L^4, C_R^4와 L^{4*}를 구한다. 그러면 3라운드 선형 근사식을 이용하여 $P_L^4[all] = L^{4*}[all]$인지를 체크 할 수 있다. 만약 $P_L^4[all] = L^{4*}[all]$을 만족한다면 추측한 다섯 번째 라운드 키를 올바른 키 후보이고 그렇지 않으면 틀린 키이다. 이러한 공격 방법을 Matsui의 알고리즘 2를 적용하여 정리하면 다음과 같다.

<공격 알고리즘>

목 표 : 32비트 5라운드 키 (K^5) 찾기.

1. 접근 방법 3에서 제시한 형태를 갖는 2^{38}개의 평문을 선택하고 대응하는 5라운드 암호문을 얻는다.

2. 추측 가능한 2^{32}개의 5라운드 키에 대해 다음 과정을 수행한다.

2.1 얻은 2^{38}개의 각각의 평문/암호문에 대해 다섯 번째 라운드를 복호화 한 후 다음 과정을 수행한다.

(a) 네 번째 라운드 출력 값 C_L^4, C_R^4와 L^{4*}를 계산한다.

(b) $L^{4*}[all]$ 값을 계산하고, $L^{4*}[all]=0$을 만족하면 T를 하나씩 증가시킨다. 여기서 T는 $L^{4*}[all]=0$을 만족하는 개수를 의미한다.

(C) $T_{\max}$($T_{\min}$)를 모든 T값들 중에 최대값(최소값)이라 하자. 그러면 다음을 통해 키비트 정보를 추측할 수 있다.

(i) 만약 $|T_{\max}-N/2|>|T_{\min}-N/2|$ 이면 키 후보를 $T_{\max}$로 채택하고

$L^{4*}[all]=P_L^4[all]$

$=P_L^1[all]\oplus K^2[all]\oplus K^3[all]=0$

으로 추측한다.($P>1/2$)

(ii) 만약 $|T_{\max}-N/2|<|T_{\min}-N/2|$ 이면 키 후보를 $T_{\min}$로 채택하고

$L^{4*}[all]=P_L^4[all]$

$=P_L^1[all]\oplus K^2[all]\oplus K^3[all]=1$

로 추측한다.($P>1/2$)

따라서, Matsui의 결과에 의해, 2^{38}개의 선택 평문을 가지고 5라운드 CIKS-1를 공격한다면 99.9% 성공 확률로 마지막 5번째 라운드 키 32비트를 찾는데 성공할 것이다.[6]

그리고, 8라운드 CIKS-1에 대한 공격도 5라운드 공격에 사용된 3라운드 선형 근사식을 이용하여 동일한 공격 방법으로 확장 할 수 있다. 다만, 32비트 키를 추측하는 것이 아니라 다섯 번째, 여섯 번째, 일곱 번째, 여덟 번째의 32비트 라운드 키 4개를 동시에 추측한다. 그러면 5라운드 공격과 마찬가지로 2^{38}개의 선택 평문을 가지고 99.9% 성공 확률로 성공할 것이다. 다만 시간 복잡도만 다를 뿐이다. [표 1]는 Matsui의 결과를 기초로 한 우리의 공격 결과를 나타낸 것이다.

〔표 1〕 공격 결과

성공 확률	78.5 %	96.7 %	99.9 %
선택 평문 수	$4\cdot\|P-(1/2)\|^{-2}$ $=2^{36}$	$8\cdot\|P-(1/2)\|^{-2}$ $=2^{37}$	$16\cdot\|P-(1/2)\|^{-2}$ $=2^{38}$
5라운드 공격에 대한 시간 복잡도	$\approx 2^{65.7}$	$\approx 2^{66.7}$	$1/5\times 2^{32}\approx 2^{38}$
8라운드 공격에 대한 시간 복잡도	$\approx 2^{164}$	$\approx 2^{165}$	$\approx 2^{166}$

Ⅳ. 결 론

지금까지 본 논문에서는 CIKS-1 알고리즘을 소개하고, CP-박스들(치환들)의 특성과 Matsui의 아이디어들을 이용하여 효율적인 선형 근사식을 제시하고 공격 알고리즘을 소개하였다. 그리고 결과로서, 99.9%의 성공 확률로 5라운드 CIKS-1암호의 마지막 라운드 키를 찾는데 약 2^{38}개의 선택 평문과 $2^{67.7}$ 정도의 암호화 시간이 요구됨을 제시하였다. 또한, 5라운드 CIKS-1 공격에 사용된 3라운드 선형 근사식을 이용하여 8라운드 CIKS-1암호로 공격을 확장할 수 있음을 보였다. 이러한 본 논문의 공격은 데이터 의존 치환들을 가지고 있는 다른 블록 암호에도 공격을 적용 할 수 있을 것이고 DDP를 가진 블록 암호 설계하는데 있어서도 본 논문의 공격 개념를 유념해야 할 것이다. 그리고, 이런 공격 방법에 대한 약점들을 해결 할 수 있다면 CIKS-1 암호는 효율성 측면에서 개선해 나갈 가치가 있다.

참 고 문 헌

[1] K. Aoki and K. Ohta, "Strict Evaluation of the Maximum Average of Differential Probability and the Maximem Average of Linear Probability", IEICE Transcations fundamentals of Elections, Communications and Computer Sciences, No. 1, 1997, pp. 2~8

[2] C. Burwick, D.C oppersmith, E. D' Avingnon, R. Gennaro et al., Proceedings of the 1st Advanced Encryption Standard Candidate Conference, Venture, California, Aug. 20-22, 1998.

[3] E. Biham and A. Shamir, "Differential Cryptanalysis of DES-like cryptosystems", *Advances in Cryptology - CRYPTO'90*, LNCS 537, Springer-Verlag, 1991, pp. 2~21.

[4] W. Becker, "Method and system for machine enciphering and deciphering", U.S. patent number 4157454, 1979.

[5] J. Borst, B. Preneel, J. Vandewalle, "Linear Cryptanalysis of RC5 and RC6", FSE'99, Springer-Verlag, 1994.

[6] Matsui, "Linear cryptanalysis method for DES cipher", Advanced in cryptology, Eurocrypt'93, Springer-Verlag, 1993.

[7] A. A. Moldovyan, N. A. Moldovyan, "A method of the cryptographical transformation of binary data blocks", Russian patent number 2141729 Bull. No. 32, 1999.

[8] A. A. Moldovyan, N. A. Moldovyan, "A cipher based on data-dependent permutations", Journal of Cryptology, Vol. 15, Num. 1, Winter 2002.

[9] J. Nakahara Jr, B. Preneel, J. Vandewalle, "Linear cryptanalysis of reduced-round versions of the SAFER", Fast Software Encryption'96, Springer-Verlag, 1996.

[10] R. L. Rivest, M. Robshow, R. Sidney, and Y. L. Yin, "The RC6 Block cipher", Proceedings of the 1st Advanced Encryption Standard Candidate Conference, Venture, California, Aug. 20-22, 1998.

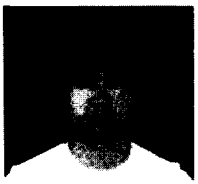
[11] B. Kaliski, Y. L. Yin, "On differential linear cryptanalysis of RC5 encryption algorithm", Advanced in cryptology, CRYPTO95, 1995.

[12] R. L. Rivest, "The RC5 encryption algorithm", Fast Software Encryption'94, Springer-Verlag, 1995.

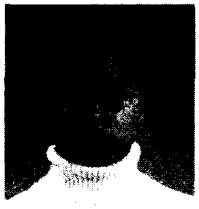
[13] Takeshi Shimoyama, Masahiko Takenaka, and Takeshi Koshiba, "Multiple Linear Cryptanalysis of a Reduced Round RC6" FSE'2002, LNCS 2365, p. 76, Springer-Verlag, 2002.

[14] Atsuko Miyaji and Masao Nonaka, "Cryptanalysis of the Reduced-Round RC6", ICICS'2002, LNCS 2513, p. 481, Springer-Verlag, 2002.

〈著者紹介〉

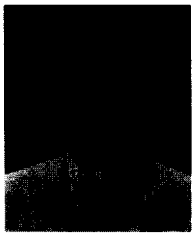


이 창 훈 (Chang-hoon Lee)
2001년 2월 : 한양대학교 수학과 학사
2003년 2월 : 고려대학교 정보보호대학원 석사
2003년 3월~현재 : 고려대학교 정보보호대학원 박사과정
<관심분야> 블록 암호 및 스트림 암호 분석 및 설계, 블록 암호 운영모드 분석 및 설계



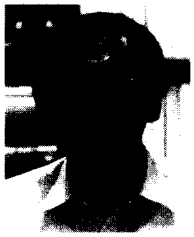
홍 득 조 (Deuk-jo Hong)
1999년 8월 : 고려대학교 수학과 학사
2001년 8월 : 고려대학교 수학과 석사
2001년 9월~현재 : 고려대학교 정보보호대학원 박사과정
<관심분야> 블록 암호 및 스트림 암호 분석 및 설계, 블록 암호 운영모드 분석 및 설계

이 성 재 (Sung-jae Lee)
1997년 8월 : 고려대학교 수학과 학사
1999년 8월 : 고려대학교 수학과 석사
1999년 9월~현재 : 한국정보보호진흥원 연구원
<관심분야> 블록 암호 및 스트림 암호 분석 및 설계



이 상 진 (Sang-jin Lee) 정회원

1987년 2월 : 고려대학교 수학과 학사
1989년 2월 : 고려대학교 수학과 석사
1994년 2월 : 고려대학교 수학과 박사
1989년 2월～1999년 2월 : 한국전자통신연구원 선임 연구원,
1999년 2월～현재 : 고려대학교 자연과학대학 부교수, 고려대학교 정보보호대학원 겸임교수, 고려대학교 정보보호기술연구센터 연구실장
<관심분야> 블록 암호 및 스트림 암호의 분석 및 설계. 암호 프로토콜, 공개키 암호 알고리즘의 분석.



양 형 진 (Hyung-jin Yang)

1990년 8월～1990년 10월 : 미국 Oak Ridge 국립 연구소. Computer Consultant
1990년 12월～1991년 12월 : 미국 신시내티대학교 박사후 연구원
1999년 1월～1999년 12월 : 미국 매릴랜드대학교 교환교수
1992년 3월～현재 : 고려대학교 자연과학대학 물리학과 교수
2001년 3월～현재 : 고려대학교 정보보호대학원 겸임교수
<관심분야> 양자암호, 암호프로토콜

임 종 인 (Jong-in Lim) 정회원

1980년 2월 : 고려대학교 수학과 학사
1982년 2월 : 고려대학교 수학과 석사
1986년 2월 : 고려대학교 수학과 박사
1999년 2월～현재 : 고려대학교 자연과학대학 정교수, 한국정보보호학회 총무이사
고려대학교 정보보호대학원 원장, 고려대학교 정보보호기술연구센터 센터장
<관심분야> 블록 암호 및 스트림 암호의 분석 및 설계, 암호 프로토콜, 공개키 암호 알고리즘의 분석, 암호정책