Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.30, NO.3, Jun. 2020 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2020.30.3.325

비트 순열 기반 블록암호의 비선형 불변 공격 저항성 연구*

정 건 상,[1†] 김 성 겸,[1] 홍 득 조,[2‡] 성 재 철,[3] 홍 석 희[4]
[1,4]고려대학교 (대학원생, 교수), [2]전북대학교 (교수), [3]서울시립대학교 (교수)

On Resistance of Bit Permutation Based Block Cipher against Nonlinear Invariant Attack*

Keonsang Jeong,[1†] Seonggyeom Kim,[1] Deukjo Hong,[2‡]
Jaechul Sung,[3] Seokhie Hong[4]
[1,4]Korea University (Graduate student, Professor),
[2]Chonbuk National University (Professor), [3]University of Seoul (Professor)

요 약

비선형 불변 공격은 비교적 간단한 구조의 키 스케줄을 갖는 경량 블록암호에서 필수적으로 고려되어야 할 공격이다. 간단한 구조의 키 스케줄을 갖는 경량 블록암호가 비선형 불변 공격에 저항성을 보이는 방법으로 가장 잘 알려진 것은 라운드 키 간의 차분 중 알려진 것들의 집합에서 선형계층에 대해 불변인 최소의 선형공간의 크기가 블록 크기와 같은지를 확인하는 것이다. 본 논문에서는 다음과 같은 연구 결과를 제시한다. 설계자 관점에서 비트 순열을 선형계층으로 사용하는 SPN 구조 경량 블록암호는 라운드 키 간의 차분의 종류가 한가지여도 비선형 불변 공격에 안전할 수 있음을 증명하고, 그러한 비트 순열의 형태와 개수를 제안한다. 또한, PRESENT 구조 블록암호는 비선형 불변 공격에 저항성을 갖기 위해 적어도 두 종류의 라운드 키 간의 차분이 필요함을 전수조사를 통해 보이며, 두 종류의 라운드 키 간의 차분을 필요로 하는 비트 순열을 사용해도 차분 공격에 대한 저항성이 오히려 증가할 수 있음을 보인다. 마지막으로 GIFT의 S-box를 사용하면서 BOGI 설계 논리를 유지하는 모든 비트 순열의 불변 성분 분포를 통해, 변형된 GIFT 구조 블록암호는 비선형 불변 공격에 저항성을 갖기 위해 적어도 8종류의 라운드 키 간의 차분이 필요함을 보인다.

ABSTRACT

Nonlinear Invariant Attack is an attack that should be considered when constructing lightweight block ciphers with relatively simple key schedule. A shortcut to prove a block cipher's resistance against nonlinear invariant attack is checking the smallest dimension of linear layer-invariant linear subspace which contains all known differences between round keys is equal to the block size. In this paper, we presents the following results. We identify the structure and number of optimal bit-permutations which require only one known difference between round keys for a designer to show that the corresponding block cipher is resistant against nonlinear invariant attack. Moreover, we show that PRESENT-like block ciphers need at least two known differences between round keys by checking all PRESENT-like bit-permutations. Additionally, we verify that

Received(03. 03. 2020), Modified(04. 24. 2020), Accepted(04. 24. 2020)
* 본 연구는 고려대 암호기술 특화연구센터(UD170109ED)를 통한 방위사업청과 국방과학연구소의 연구비 지원으로 수행되었습니다.
* 본 논문은 2019년도 동계 학술대회에 발표한 우수논문을 개선 및 확장한 것임
† 주저자, pooh4572@korea.ac.kr
‡ 교신저자, deukjo.hong@jbnu.ac.kr(Corresponding author)

the variants of PRESENT-like bit-permutations requiring the only two known differences between round keys do not conflict with the resistance against differential attack by comparing the best differential trails. Finally, through the distribution of the invariant factors of all bit-permutations that maintain BOGI logic with GIFT S-box, GIFT-variant block ciphers require at least 8 known differences between round keys for the resistance.

Keywords: Nonlinear Invariant Attack, Bit Permutation, Round Key, PRESENT, GIFT

I. 서 론

경량 디바이스의 암호화 서비스 수요가 증가하면서 새로운 경량 블록암호가 지속적으로 제안되고 있다. 경량 블록암호는 경량성을 설계 목표로 하여 주로 단순한 키 스케줄 또는 마스터키로부터 부가 연산을 최소화하여 그대로 사용하는 경향이 있다. 하지만 단순한 구조의 키 스케줄에 대한 구조적 취약성으로 인해 2016년에 새로운 공격인 비선형 불변 공격이 제안되어 Midori, iSCREAM의 안전성이 재조명되었다[1]. 비선형 불변 공격은 취약키(weak-key) 가정하에 한 라운드의 비선형 불변을 임의의 라운드의 비선형 불변으로 확장할 수 있다. 즉, 차분 공격, 선형 공격과는 달리 취약키 가정하에 블록암호의 라운드 수와 관계없이 공격을 수행할 수 있다. 따라서 복잡한 구조의 키 스케줄을 사용할 경우, 이러한 취약키 집합을 찾기가 어려우므로, 비교적 간단한 구조의 키 스케줄(마스터 키에 라운드 상수를 더하여 라운드 키를 생성하는 방식 등)을 갖는 경량 블록암호에 주로 적용된다. 이로 인해 비교적 간단한 구조의 키 스케줄을 갖는 경량 블록암호에서는 필수적으로 고려되어야 할 공격이다.

설계자 관점에서 비선형 불변 공격에 저항성을 보이는 방법이 2017년에 제안되었다[2]. [2]에서는 라운드 키 간의 차분 중 알려진 것들의 집합에서 선형계층에 대해 불변인 최소의 선형공간의 크기가 클수록 비선형 불변 공격에 저항성을 보일 수 있음을 증명하였다. 또한, 주어진 선형계층에 대해 비선형 불변 공격에 저항성을 갖는 라운드 키 간의 차분의 최소 개수를 보였다. 라운드 키 간의 차분의 종류가 한가지여도 비선형 불변 공격에 저항성을 보일 수 있는 선형계층을 사용하면, 어떠한 구조의 키 스케줄을 사용하여도 비선형 불변 공격에 안전하다.

본 논문에서는 설계자 관점에서 라운드 키 간의 차분의 종류가 한가지여도 비선형 불변 공격에 저항성을 갖는 비트 순열의 형태와 개수를 제안한다. 비트 순열을 선형계층으로 사용하는 경우, 해당 비트 순열에 대응되는 순환행렬의 최소다항식과 특성다항식이 같으면 라운드 키 간의 차분의 종류가 한가지여도 비선형 불변 공격에 저항성을 갖는다. 이러한 특성을 만족하는 비트 순열을 ***최적의 비트 순열***이라 표기한다. 또한, PRESENT 구조 블록암호는 비선형 불변 공격에 저항성을 갖기 위해 적어도 두 종류의 라운드 키 간의 차분이 필요함을 전수조사를 통해 보이며, 두 종류의 라운드 키 간의 차분을 필요로 하는 비트 순열을 사용해도 차분 공격에 대한 저항성이 오히려 증가할 수 있음을 보인다. 마지막으로 GIFT의 S-box를 사용하면서 BOGI 설계 논리를 유지하는 모든 비트 순열의 불변 성분 분포를 통해, 변형된 GIFT 구조 블록암호는 비선형 불변 공격에 저항성을 갖기 위해 적어도 8종류의 라운드 키 간의 차분이 필요함을 보인다.

본 논문의 구성은 다음과 같다. Ⅱ장에서는 표기법과 비선형 불변 공격, 해당 공격에 대한 저항성 입증 방법을 설명한다. Ⅲ장에서는 최적의 비트 순열 도출 방법에 관해 기술하고, 경량 블록암호에 적용하여 도출한 결과를 Ⅳ장에서 제시한다. 끝으로 Ⅴ장에서 결론을 맺는다.

II. 배경 지식

2.1 표기법

본 논문에서 사용된 표기법은 다음과 같다.

- n : 블록암호의 블록 비트 크기
- L : SPN 구조의 선형계층, L-Layer
- S : SPN 구조의 비선형계층, S-Layer
- π : 비트 순열
- P_π : 비트 순열 π에 대응되는 순환행렬 (permutation matrix)
- $(i_1 i_2 \cdots i_k)$: 위수가 k인 사이클 γ
  $\begin{cases}\gamma(i_1)=i_2, \gamma(i_2)=i_3, \cdots, \gamma(i_k)=i_1 \\ \gamma(i)=i, \forall i \notin \{i_1, i_2, \cdots, i_k\}\end{cases}$

모든 비트 순열(π)은 대응되는 순환행렬(P_π)이 존

재하고, 사이클들의 조합으로 나타낼 수 있다.

$$\text{ex) } \pi=\begin{pmatrix}1&2&3&4&5\\1&4&2&5&3\end{pmatrix}\Leftrightarrow P_\pi=\begin{bmatrix}1&0&0&0&0\\0&0&0&1&0\\0&1&0&0&0\\0&0&0&0&1\\0&0&1&0&0\end{bmatrix}\Leftrightarrow(1)(2453)$$

- $C(Q_i)$: 다항식 Q_i에 대한 동반행렬(companion matrix)
- $A\sim B$: $A\sim B$ if $\exists P\, s.t.\, P^{-1}AP=B$
- $\chi_A(x)$: 행렬 A의 특성다항식(characteristic polynomial)

$n\times n$행렬 A의 특성다항식은 $\chi_A(x)=\det(xI-A)$이다. 이때 I는 $n\times n$단위행렬(identity matrix)이다.

- $m_A(x)$: 행렬 A의 최소다항식(minimal polynomial)

행렬 A의 최소다항식은 최고차항의 계수가 1인 다항식으로 다음을 만족하는 최소 차수(d) 다항식이다.

$$m_A(x)=\sum_{i=0}^{d}p_ix^i\in F_2[x]\, s.t.\, m_A(A)=\sum_{i=0}^{d}p_iA^i=0$$

2.2 비선형 불변

비선형 불변 공격은 블록암호 $E_k:F_2^n\rightarrow F_2^n$의 비선형 불변을 이용한 공격으로 비선형 불변은 다음과 같이 정의한다.

정의 1[1]. 블록암호 $E_k:F_2^n\rightarrow F_2^n$에 대해, 불함수 $g:F_2^n\rightarrow F_2$가 $g(x)+g(E_k(x))=Const, \forall x\in F_2^n$을 다수의 키 k에 대해 만족시킬 때, g를 E_k의 비선형 불변이라 하고, 이를 만족하는 k는 비선형 불변 g에 대한 취약키(weak-key)라고 한다.

블록암호의 비선형 불변이 존재하는 경우에는 구별 공격, 평문 복원 및 키 복원을 시행할 수 있음이 2016년에 비선형 불변 공격을 통해 알려졌다[1]. 2018년에는 확장된 비선형 불변 공격이 제안되어 구별 공격을 시행하였다[4]. 또한, [6]에서는 correlation matrix를 통해 비선형 불변을 도출하고, 포화 공격(integral attack)과 결합하여 키 복원을 시행하였다.

2.3 비선형 불변 공격의 저항성 입증방법

본 논문에서는 Fig. 1.과 같이 SPN 구조의 블록암호에 대해 살펴본다.

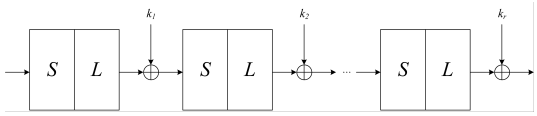

Fig. 1. SPN with S-Layer S and linear layer L

정의 2[2]. 불함수 g의 선형구조(linear structure)는 다음을 만족하는 원소 $\alpha\in F_2^n$를 뜻한다.

$$LS(g):=\{\alpha\in F_2^n\,|\,g(x)+g(x+\alpha)=Const, \forall x\in F_2^n\}$$

이때 선형구조에 속한 모든 원소 α를 모으면 F_2^n의 부분 선형공간(linear subspace)이고, 이를 g의 선형공간(linear space)이라 한다.

블록암호의 비선형 불변을 도출하기 위해서는 한 라운드에 대한 비선형 불변을 구해야 한다. 하지만 이는 현실적으로 구하기 어려우므로 비선형계층인 S-Layer와 선형 부분인 $Add_{k_i}\circ L$에 공통으로 존재하는 비선형 불변을 블록암호의 비선형 불변으로 도출한 후, 이를 활용하여 공격을 진행한다. 이때 서로 다른 라운드의 선형부분에 공통으로 존재하는 비선형 불변의 선형공간에 대한 특징은 다음과 같다.

정리 1[2]. 불함수 g가 라운드 키로 k_i, k_j를 사용하는 선형부분 $Add_{k_i}\circ L, Add_{k_j}\circ L$의 비선형 불변일 때, $LS(g)$는 k_i+k_j를 포함하며, L에 대해 불변인 선형공간이다.

정리 1에 의해 라운드 키 간의 차분은 $LS(g)$에 포함된다. 이때 선형계층 L에 대해 불변인 선형공간 중 $c(\in F_2^n)$를 포함하는 최소의 선형공간을 $W_L(c)$로 정의하면, 보조정리 1을 통해 구할 수 있다. 보조정리 1에서 〈 〉 표기는 선형생성(linear span)을 의미한다.

보조정리 1[2]. $W_L(c) = \langle L^i(c), i \geq 0 \rangle$

또한, 라운드 키 간의 차분 중 알려진 것들의 집합을 D로 정의하고, D를 포함한 최소 선형공간인 $W_L(D)$는 다음과 같이 정의한다.

$$W_L(D) := \sum_{c \in D} \langle L^i(c), i \geq 0 \rangle = \sum_{c \in D} W_L(c)$$

블록암호가 비선형 불변 공격에 저항성을 갖는다는 것은 비선형 불변 g가 상수함수인 **0,1**로만 존재할 경우이다. 비선형 불변 공격에 대한 저항성은 $W_L(D)$의 차원을 통해 입증할 수 있다.

정리 2[2, 7]. 불함수 g와 $LS(g)$는 다음의 필요충분조건을 갖는다.

$$\dim LS(g) \geq d \Leftrightarrow \deg(g) \leq \begin{cases} n-d & \text{if } d \neq n \\ 1 & \text{if } d = n \end{cases}$$

보조정리 2[2]. $W_L(D) \subseteq LS(g)$

정리 2와 보조정리 2를 통해 $\dim W_L(D) = n$일 경우, 비선형 불변 g는 선형함수 또는 상수함수이다. 비선형계층 S에서 비선형 불변 g가 선형함수일 경우에는 S-Layer에서 확률이 1인 선형 근사식이 존재한다. 하지만 S-Layer에서 확률이 1인 선형 근사식이 존재하는 S-box를 사용하지 않으므로 $W_L(D)$의 차원이 블록 크기와 같을 때, 해당 블록암호는 비선형 불변 공격에 저항성을 갖는다.

2.4 비선형 불변 공격의 저항성과 라운드 키 간의 차분 과의 관계

비선형 불변 공격의 저항성을 $W_L(D)$의 차원을 통해 보일 수 있고, 선형계층 L이 주어진 경우 $W_L(D)$의 차원이 블록 크기와 같게 되는 라운드 키 간의 차분의 최소 개수가 정해진다. 이는 선형계층 L에 대한 Rational Canonical Form의 불변 성분의 개수와 같다[2, 3]. Fig. 2.는 선형계층 L에 대한 Rational Canonical Form을 나타내며, 이 때 다항식 Q_i를 L의 불변 성분(invariant factors)이라 부른다. 또한, $Q_1 = m_L(x)$, $Q_1 \cdot Q_2 \cdot \cdots \cdot Q_r = \chi_L(x)$, $Q_r | Q_{r-1} | \cdots | Q_1$이 성립한다.

$$\begin{pmatrix} C(Q_r) & & & \\ & C(Q_{r-1}) & & \\ & & \ddots & \\ & & & C(Q_1) \end{pmatrix}$$

Fig. 2. Linear Layer L's Rational Canonical Form

정리 3[2]. $Q_1, \cdots, Q_r$이 선형계층 L의 불변 성분이고 $t \leq r$이면,

$$\max_{c_1, \cdots, c_t} \dim W_L(c_1, \cdots, c_t) = \sum_{i=1}^{t} \deg Q_i$$

정리 3에 의해 다음과 같은 따름정리를 얻는다.

따름정리 1. 라운드 키 간의 차분의 종류가 한가지여도 $\dim W_L(c_1) = n$이 성립하려면 선형계층 L의 최소다항식과 특성다항식이 같아야 한다. 즉, 선형계층 L의 불변 성분이 하나인 것과 $\chi_L(x) = m_L(x)$은 동치이다.

III. 최적의 비트 순열의 형태와 개수 도출

본 장에서는 선형계층 중 최적의 비트 순열의 형태와 개수를 도출한다. 최적의 비트 순열 π는 $\chi_{P_\pi}(x) = m_{P_\pi}(x)$가 성립하는 비트 순열을 뜻한다. 최적의 비트 순열을 사용하면, 라운드 키 간의 차분의 종류가 한가지여도 비선형 불변 공격에 저항성을 갖는다.

정리 4[3]. 행렬 A, B에 대해 $A \sim B$이면 $\chi_A(x) = \chi_B(x), m_A(x) = m_B(x)$이다.

정리 5. 모든 P_{π_i}에 대해, π_i를 구성하는 사이클의 개수와 각 사이클 내 위수가 같으면서 순서가 정렬된 $P_{\pi_j} (= P^{-1} P_{\pi_i} P)$로 변환하는 행렬 P가 존재하고 $P_{\pi_i} \sim P_{\pi_j}$이다.

증명. 선형대수학에서의 기저 변환(basis change)을 통해 자명하게 보일 수 있다. □

예시. 주어진 비트 순열(π_1)에 대해 사이클의 순서가 정렬된 비트 순열(π_2)로 변환하는 행렬 P는 아래와 같다. 이는 4를 2로, 2를 4로 바꿔주면 된다.

$$\pi_1=\begin{pmatrix}1&2&3&4&5\\4&5&1&3&2\end{pmatrix}\Leftrightarrow P_{\pi_1}=\begin{bmatrix}0&0&0&1&0\\0&0&0&0&1\\1&0&0&0&0\\0&0&1&0&0\\0&1&0&0&0\end{bmatrix}\Leftrightarrow(143)(25)$$

$$\pi_2=\begin{pmatrix}1&2&3&4&5\\2&3&1&5&4\end{pmatrix}\Leftrightarrow P_{\pi_2}=\begin{bmatrix}0&1&0&0&0\\0&0&1&0&0\\1&0&0&0&0\\0&0&0&0&1\\0&0&0&1&0\end{bmatrix}\Leftrightarrow(123)(45)$$

$$\exists P=\begin{bmatrix}1&0&0&0&0\\0&0&0&1&0\\0&0&1&0&0\\0&1&0&0&0\\0&0&0&0&1\end{bmatrix} s.t. P_{\pi_2}=P^{-1}P_{\pi_1}P$$

정리 5에 의해 모든 비트 순열은 사이클 내 원소의 순서가 정렬된 비트 순열로 변환되고, 두 비트 순열에 대응되는 순환행렬의 닮음과 정리 4에 의해 이들의 최소다항식과 특성다항식은 각각 같다. 따라서 모든 비트 순열에 대해 두 식이 같은 비트 순열을 찾지 않고, 정렬된 비트 순열에 대해 두 식이 같은 비트 순열을 찾는 것만으로도 충분하다.

최적의 비트 순열의 형태와 개수 도출방법은 다음과 같다. 정리 4, 5에 의해 모든 비트 순열을 살펴보지 않고 정렬된 비트 순열만을 살펴봐도 충분하고, 정렬된 비트 순열은 해당 비트 순열이 하나의 사이클로 구성된 경우와 두 개 이상의 사이클로 구성된 경우로 나눌 수 있다. 3.1절에서는 정렬된 비트 순열이 하나의 사이클로 구성된 경우 최소다항식과 특성다항식이 같을 수 있는지를 파악하고, 3.2절에서는 정렬된 비트 순열이 두 개 이상의 사이클로 구성된 경우 두 식이 같을 수 있는지를 파악한다.

3.1 비트 순열이 하나의 사이클로 구성된 경우

보조정리 3[3]. 동반행렬 $C(Q_i)$는 $m_{C(Q_i)}(x)=\chi_{C(Q_i)}(x)=Q_i$를 만족한다.

정리 6. 비트 순열이 하나의 사이클로 구성된 경우, 해당 순환행렬의 최소다항식과 특성다항식이 같고, 그 개수는 $(n-1)!$개다.

증명. 정리 5에 의해 하나의 사이클로 구성된 모든 비트 순열을 대표하는 사이클은 $(12\cdots n)$으로 표현된다. 이를 순환행렬로 표현하면 동반행렬의 특별한 형태이다.

$$\pi=\begin{pmatrix}1&2&\cdots&n\\2&3&\cdots&1\end{pmatrix}\Leftrightarrow P_\pi=\begin{bmatrix}0&1&&&\\&0&1&&\\&&\ddots&\ddots&\\&&&0&1\\1&&&&0\end{bmatrix}\Leftrightarrow(12\cdots n)$$

따라서 보조정리 3에 의해 $m_{P_\pi}(x)=\chi_{P_\pi}(x)=x^n-1$이고, 그 개수는 원순열의 개수와 같으므로 $(n-1)!$개다. □

3.2 비트 순열이 여러 개의 사이클로 구성된 경우

보조정리 4[3]. 블록 행렬 $M=\begin{bmatrix}M_1&&&\\&M_2&&\\&&\ddots&\\&&&M_r\end{bmatrix}$의 최소다항식은 각 블록인 $M_i(i=1,\cdots,r)$의 최소다항식들의 최소공배수와 같다.

정리 7. 비트 순열이 여러 개의 사이클로 구성된 경우, 해당 순환행렬의 최소다항식과 특성다항식은 같지 않다.

증명. 정리 5에 의해 여러 개의 사이클로 구성된 모든 비트 순열을 대표하는 사이클은 $(12\cdots i_1)(i_1+1\cdots i_1+i_2)\cdots(n-i_k+1\cdots n)$으로 표현된다. 전체 사이클에 대응되는 비트 순열을 π, 각 사이클에 대응되는 비트 순열을 $\pi_1,\cdots,\pi_k$로 표현하면 다음과 같다.

$$\pi_1=\begin{pmatrix}1&2&\cdots&i_1\\2&3&\cdots&1\end{pmatrix},\cdots,\pi_k=\begin{pmatrix}n-i_k+1&\cdots&&n\\n-i_k+2&\cdots&n-i_k+1\end{pmatrix}$$

$$\pi=\begin{pmatrix}1&2&\cdots&i_1&\cdots&n-i_k+1&\cdots&n-1&n\\2&3&\cdots&1&\cdots&n-i_k+2&\cdots&n&n-i_k+1\end{pmatrix}$$

이때 P_π는 대각 성분이 동반행렬로 이루어진 블록행렬로,

$$P_\pi=\begin{bmatrix}P_{\pi_1}&&&\\&P_{\pi_2}&&\\&&\ddots&\\&&&P_{\pi_k}\end{bmatrix}\quad(1)$$

이고 $P_{\pi_1}, \cdots, P_{\pi_k}$는 크기가 각각 $i_1 \times i_1, \cdots, i_k \times i_k$이며 $i_1 + i_2 + \cdots + i_k = n$이 성립한다. 또한, $P_{\pi_1}, \cdots, P_{\pi_k}$의 최소다항식은 각각 $x^{i_1}-1, \cdots, x^{i_k}-1$이고, 보조정리 4에 의해 $m_{P_\pi}(x) = lcm(m_{P_{\pi_1}}(x), \cdots, m_{P_{\pi_k}}(x))$이다. 이때 $P_{\pi_1}, \cdots, P_{\pi_k}$의 최소다항식들은 공통인수로 $x-1$을 가지므로, P_π의 최소다항식의 차수는 n보다 낮다. 하지만 P_π의 특성다항식의 차수는 n이므로 P_π의 최소다항식과 특성다항식은 같지 않다. □

예시. 비트 순열이 사이클 (165)(27)(384)로 이루어진 경우, 정리 5에 의해 사이클 내 원소의 순서가 정렬된 사이클 (123)(45)(678)로 변환된다. 이는 6을 2로, 5를 3으로, 2를 4로, 7을 5로, 3을 6으로, 8을 7로, 4를 8로 바꿔주면 된다. 이때 정렬된 사이클에 대응되는 순환행렬은 아래와 같다.

$$P_\pi = \begin{bmatrix} 0\,1\,0 & & \\ 0\,0\,1 & & \\ 1\,0\,0 & & \\ & 0\,1 & \\ & 1\,0 & \\ & & 0\,1\,0 \\ & & 0\,0\,1 \\ & & 1\,0\,0 \end{bmatrix}$$

정리 6, 7에 의해 라운드 키 간의 차분의 종류가 한가지여도 비선형 불변 공격에 저항성을 갖는 비트 순열의 형태는 하나의 사이클로 구성되어야 하고, 그 개수는 $(n-1)!$개이다. 즉, 하나의 사이클로 구성된 비트 순열이 최적의 비트 순열이고, 해당 비트 순열을 사용할 경우 라운드 키 간의 차분의 종류가 한가지여도 비선형 불변 공격에 저항성을 갖는다. 또한, 앞선 정리들로 다음과 같은 따름정리를 얻는다.

따름정리 2. 비트 순열을 구성하는 각 사이클 내 위수를 크기가 큰 순으로 정렬한 것을 $a_1, a_2, \cdots, a_k$라 하자. 만약 $a_k | a_{k-1} | \cdots | a_1$이 성립하면, 불변 성분의 개수와 차수는 비트 순열을 구성하는 사이클의 개수와 사이클 내 위수와 동일하다.

증명. 모든 비트 순열을 (1)과 같이 표현할 수 있고, 동반행렬의 Rational Canonical Form은 동반행렬과 같다. 또한, Rational Canonical Form은 동반행렬들의 direct sum이기 때문에, 불변 성분의 개수와 차수는 비트 순열을 구성하는 사이클의 개수와 사이클 내 위수와 동일하다. □

따름정리 2를 통해 비트 순열의 경우, Rational Canonical Form을 통해 불변 성분을 구하지 않고도 비트 순열의 사이클을 통해 불변 성분의 개수와 차수를 파악할 수 있다.

IV. 실제 경량 블록암호에 적용

본 장에서는 Ⅲ장에서 구한 최적의 비트 순열과 기존의 경량 블록암호 중 비트 순열을 선형계층으로 갖는 PRESENT[8], GIFT[9]를 비교한다. 또한, 최적의 비트 순열을 PRESENT의 설계 논리에 따라 적용한 결과를 보인다. 즉, 하나의 사이클로 구성된 비트 순열이 PRESENT 구조에 존재하는지를 전수조사를 통해 확인한다. 마지막으로 GIFT의 S-box를 사용하면서 BOGI 설계 논리를 유지하는 모든 비트 순열의 불변 성분 분포를 보인다.

4.1 최적의 비트 순열과 PRESENT, GIFT 비교

PRESENT 비트 순열의 경우, 위수가 1인 사이클 4개, 위수가 3인 사이클 20개로 총 24개의 사이클로 구성된다. 따름정리 2를 통해 PRESENT는 24개의 불변 성분을 가지며 차수가 1인 불변 성분 4개, 차수가 3인 불변 성분 20개를 갖는 것을 알 수 있다. PRESENT 비트 순열에서 도출한 불변 성분은 다음과 같다.

$$Q_1(X) = \cdots = Q_{20}(X) = (X+1)(X^2+X+1)$$
$$Q_{21}(X) = \cdots = Q_{24}(X) = X+1$$

이는 정리 3에 의해 설계 관점에서 최소 24종류의 라운드 키 간의 차분으로 비선형 불변 공격에 저항성을 보일 수 있음을 뜻한다.

GIFT 비트 순열의 경우, 위수가 1인 사이클 4개, 위수가 2인 사이클 2개, 위수가 4인 사이클 14개로 총 20개의 사이클로 구성된다. 이를 통해 GIFT는 20개의 불변 성분을 가지며 차수가 1인 불변 성분 4개, 차수가 2인 불변 성분 2개, 차수가 4인 불변 성분 14개를 갖는 것을 알 수 있다. GIFT 비트 순열에서 도출한 불변 성분은 다음과 같다.

$$Q_1(X) = \cdots = Q_{14}(X) = (X+1)^4$$
$$Q_{15}(X) = Q_{16}(X) = (X+1)^2$$
$$Q_{17}(X) = \cdots = Q_{20}(X) = X+1$$

이는 설계 관점에서 최소 20종류의 라운드 키 간의 차분으로 비선형 불변 공격에 저항성을 보일 수 있음을 뜻한다.

Ⅲ장에서 구한 최적의 비트 순열의 형태는 하나의 사이클로 구성되므로 1개의 불변 성분을 갖는다. 최적의 비트 순열에서 도출한 불변 성분은 다음과 같다.

$$Q_1(X) = (X+1)^{64}$$

이는 설계 관점에서 라운드 키 간의 차분의 종류가 한가지여도 비선형 불변 공격에 저항성을 보일 수 있음을 뜻한다.

최적의 비트 순열과 PRESENT, GIFT 선형계층의 불변 성분 개수를 정리하면 Table 1.과 같다.

Fig. 3.은 라운드 키 간의 차분의 개수에 따른 $W_L(c_1, \cdots, c_t)$의 최대 차원을 나타낸 그래프이다. $W_L(c_1, \cdots, c_t)$의 최대 차원은 선형계층의 불변 성분들의 차수만큼 증가한다. 최적의 비트 순열의 경우 라운드 키 간의 차분의 종류가 한가지여도 $W_L(c_1)$의 최대 차원이 블록 크기인 64와 같고, PRESENT, GIFT의 경우 각각 최소 24종류, 20종류의 라운드 키 간의 차분으로 $W_L(c_1, \cdots, c_{24})$, $W_L(c_1, \cdots, c_{20})$의 최대 차원이 블록 크기인 64와 같다.

Table 1. Comparison table of Optimal L-Layer, PRESENT L-Layer and GIFT L-Layer

	Optimal L-Layer	PRESENT L-Layer	GIFT L-Layer
Number of Invariant Factors	1	24	20

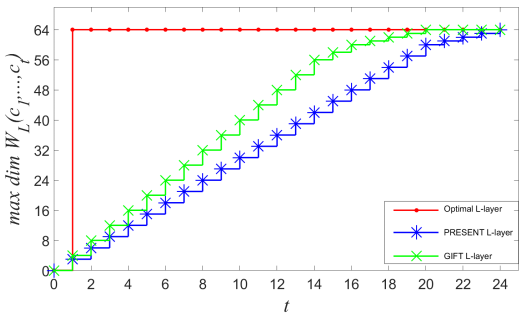

Fig. 3. For Optimal $L-$Layer, PRESENT $L-$Layer and GIFT $L-$Layer, this figure shows the highest possible dimension of $W_L(c_1, \cdots, c_t)$ for t values $c_1, \cdots, c_t$ (see Theorem 3)

4.2 최적의 비트 순열 적용 : PRESENT

PRESENT는 16비트 순열로부터 설계 논리에 맞게 확장한 64비트 순열을 사용한다. Fig. 4.와 같이 16개의 S-box를 4개씩 나눈 뒤 이를 각각 그룹이라 지칭하고, 설계 논리에 따라 비트 순열을 확장한다. PRESENT의 설계 논리를 살펴보면 다음과 같다.

1. S-box의 입력 비트는 동일한 그룹의 4개의 서로 다른 S-box로부터 선택된다.
2. 한 그룹의 4개의 S-box에 대한 입력 비트는 16개의 서로 다른 S-box로부터 선택된다.
3. 특정 S-box에 대한 4개의 출력 비트는 다음 라운드에서 각각 다른 그룹의 4개의 S-box의 입력 비트로 보낸다.
4. 다른 그룹에 속하는 S-box의 출력 비트는 서로 다른 S-box의 입력 비트로 보낸다.

본 논문에서는 동일한 설계 논리를 갖는 비트 순열을 탐색한 결과, 하나의 사이클로 구성된 비트 순열이 존재하지 않음을 전수조사를 통해 확인하였다. 즉, PRESENT와 동일한 설계 논리를 갖는 암호의 경우 비선형 불변 공격에 저항성을 가지려면 적어도 두 종류의 라운드 키 간의 차분이 필요하다.

PRESENT의 설계 논리를 따르며, 두 종류의 라운드 키 간의 차분을 필요로 하는 비트 순열로 변경한 PRESENT를 Var-PRESENT라 표기한다. Var-PRESENT에 적용한 비트 순열을 대표적으로 3가지만 나타내면 Fig. 5.와 같다. PRESENT 비트 순열은 24개의 사이클로 구성되는 반면 Var-PRESNET 비트 순열은 2개의 사이클로 구성

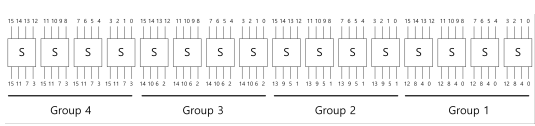

Fig. 4. Grouping of S-boxes in PRESENT

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
$P_1(i)$	0	17	33	49	2	18	34	50	1	19	35	51	3	16	32	48	4	21	37	53	6	22	38	54	5	23	39	55	7	20	36	52
$P_2(i)$	1	18	35	49	0	19	33	50	3	17	51	32	2	16	48	34	5	22	39	53	4	23	37	54	7	21	55	36	6	20	52	38
$P_3(i)$	2	17	32	50	1	16	33	48	0	19	35	49	3	18	51	34	6	21	36	54	5	20	37	52	4	23	39	53	7	22	55	38
i	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
$P_1(i)$	8	25	41	57	10	26	42	58	9	27	43	59	11	24	40	56	12	29	45	61	14	30	46	62	13	31	47	63	15	28	44	60
$P_2(i)$	9	26	43	57	8	27	41	58	11	25	59	40	10	24	56	42	13	30	47	61	12	31	45	62	15	29	63	44	14	28	60	46
$P_3(i)$	10	25	40	58	9	24	41	56	8	27	43	57	11	26	59	42	14	29	44	62	13	28	45	60	12	31	47	61	15	30	63	46

Fig. 5. Bit permutation applied to Var-PRESENT, bit i is moved to bit position $P(i)$

된다.

Fig. 6.은 PRESENT와 Var-PRESENT의 차분 공격에 대한 저항성 비교결과이다. 차분 공격에 대한 저항성은 차분 경로의 최대 확률이 2^{-64}보다 작아지는 라운드를 측정한 결과이다. PRESENT의 경우, 차분 공격과 비선형 불변 공격에 저항성을 갖기 위해서는 각각 최소 15라운드와 최소 24종류의 라운드 키 간의 차분이 필요하다. Var-PRESENT의 경우, 차분 공격과 비선형 불변 공격에 저항성을 갖기 위해서는 각각 최소 13라운드와 최소 2종류의 라운드 키 간의 차분이 필요하다. 이에 대한 정리는

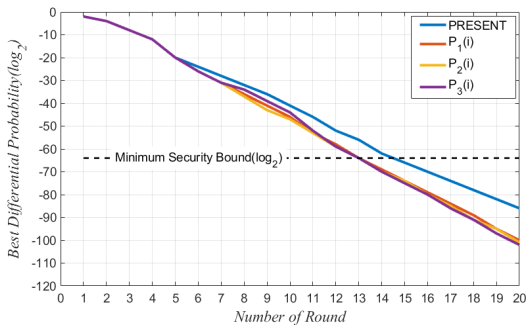

Fig. 6. Best differential trail's probabilities of PRESENT and Var-PRESENT

Table 2. Comparison table between PRESENT and Var-PRESENT

	Resistance against Differential Attack	Resistance against Nonlinear Invariant Attack
PRESENT	15 round	24 known differences between round keys
Var-PRESENT	13 round	2 known differences between round keys

Table 2.와 같다.

Var-PRESENT를 탐색하여 차분 공격과 비선형 불변 공격에 대한 저항성을 확인한 결과, PRESENT보다 적은 라운드와 적은 라운드 키 간의 차분의 종류를 통해 공격에 저항성을 보일 수 있음을 확인하였다.

4.3 BOGI

경량 블록암호의 설계 논리 중 하나인 BOGI는 GIFT에서 처음 소개되었다[9]. BOGI는 비트 순열을 선형계층으로 갖는 경우에 적용할 수 있는 설계 논리로, S-box의 출력 차분의 활성 비트 수가 1개일 경우(Bad-Output), 비트 순열을 통과 후 다음 S-box의 출력 차분의 활성 비트 수가 2개 이상이 나오는 입력 차분(Good-Input)을 만드는 방법이다. 따라서 S-box의 브랜치 넘버가 2임에도 1비트에서 1비트로 계속 이어지는 차분, 선형 특성을 만들 수 없게 된다. BOGI 설계 논리의 자세한 내용은 [9]를 참고하길 권장한다.

BOGI 설계 논리를 만족하는 함수 π를 설계하는 방법은 다음과 같다. 이때 GI, GO, BI, BO는 각각 Good Input, Good Output, Bad Input, Bad Output을 의미하며, 1-1비트 DDT, LAT에서 GI는 행을 기준으로 원소가 모두 0인 것을 말하고, BI는 적어도 하나는 0이 아닌 것을 의미한다. 마찬가지로 GO와 BO는 열을 기준으로 위와 같은 조건을 적용한 것이다. 먼저 $\pi_a : BO \rightarrow GI$를 정의하면 $|BO| \leq |GI|$이므로 단사함수이다. 이때 π_a는 "Bad Output must go to Good Input"을 보장한다. 같은 논리로 $\pi_b : GO \rightarrow \pi_a(BO)^C$를 정의하면 단사함수이다. π_a와 π_b를 통합한 $\pi : BO \cup GO \rightarrow BI \cup GI$를 $e \in BO$이면 $\pi(e) = \pi_a(e)$, $e \in GO$이면 $\pi(e) = \pi_b(e)$로 정의하면 π는 BOGI 기법을 만족한다. GIFT의 경우,

1-1비트 DDT, LAT는 Table 3., Table 4.와 같고, $\pi_a : \{2,3\} \rightarrow \{2,3\}, \pi_b : \{0,1\} \rightarrow \{0,1\}$이며 이들을 통합한 π는 다음과 같다.

- $\pi(0)=0, \pi(1)=1, \pi(2)=2, \pi(3)=3$

Table 3. GIFT 1-1 bit DDT

Δx \ Δy	0001(**0**)	0010(**1**)	0100(**2**)	1000(**3**)
0001(**0**)	0	0	0	2
0010(**1**)	0	0	0	0
0100(**2**)	0	0	0	0
1000(**3**)	0	0	0	0

Table 4. GIFT 1-1 bit LAT

Δx \ Δy	0001(**0**)	0010(**1**)	0100(**2**)	1000(**3**)
0001(**0**)	0	0	2	4
0010(**1**)	0	0	0	2
0100(**2**)	0	0	0	0
1000(**3**)	0	0	0	0

4.4 최적의 비트 순열 적용 : GIFT

GIFT는 PRESENT와는 달리 BOGI를 활용하여 비트 순열을 구성한다. GIFT의 S-box를 사용하면서 BOGI 설계 논리를 만족하는 π함수가 총 4개 존재하고, 이를 각각 $\pi_1, \pi_2, \pi_3, \pi_4$라 표기하면 다음과 같다.

- $\pi_1(0)=0, \pi_1(1)=1, \pi_1(2)=2, \pi_1(3)=3$
- $\pi_2(0)=0, \pi_2(1)=1, \pi_2(2)=3, \pi_2(3)=2$
- $\pi_3(0)=1, \pi_3(1)=0, \pi_3(2)=2, \pi_3(3)=3$
- $\pi_4(0)=1, \pi_4(1)=0, \pi_4(2)=3, \pi_4(3)=2$

또한, i번째 라운드의 S-box를 $Sb_0^i, \cdots, Sb_{15}^i$로 표기하고 이들을 2개의 그룹인 몫($Qx$)과 나머지($Rx$) 그룹으로 나누면 다음과 같다.

- $Qx = \{Sb_{4x}, Sb_{4x+1}, Sb_{4x+2}, Sb_{4x+3}\}$
- $Rx = \{Sb_x, Sb_{4+x}, Sb_{8+x}, Sb_{12+x}\}, where\, 0 \le x \le 3$

이때 Qx^i에서 Rx^{i+1}로 가는 BOGI 비트 순열을 표현하면 Table 5.와 같고, Table 5.에서 π를 π_1으로 사용할 경우 GIFT의 16비트 순열로 Fig. 8.과 같다. 또한, GIFT의 64비트 순열은 Fig. 7.과 같이 표현된다. 이때 BOGI Bit-Permutation은 Fig. 8.의 16비트 순열이다.

BOGI 설계 논리를 유지하는 비트 순열의 개수는 각 π함수마다 크기 4의 라틴 방진 개수인 576개다. 이는 Table 5.의 원소들이 각 행과 열에 모두 중복되지 않는 경우의 수이다. 이를 통해 GIFT의 S-box를 사용하면서 BOGI 설계 논리를 유지하는 모든 비트 순열의 개수는 2304개임을 알 수 있다. 또한, 이들의 불변 성분의 분포를 살펴보면 Table 6.과 같다. Table 6.을 통해 GIFT 구조 블록암호의 경우, 불변 성분 개수의 최솟값이 8임을 알 수 있다. 이는 BOGI 설계 논리를 만족하는 함수인 π를 π_4로 사용할 경우, 8개의 불변 성분을 갖는 비트 순열이 288개가 있음을 뜻한다. 또한, 변형된 GIFT 구조 블록암호는 비선형 불변 공격에 저항성을 갖기 위해 적어도 8종류의 라운드 키 간의 차분

Table 5. BOGI bit-permutation mapping from Qx^i to Rx^{i+1}

Qx^i \ Rx^{i+1}	Sb_x^{i+1}	Sb_{4+x}^{i+1}	Sb_{8+x}^{i+1}	Sb_{12+x}^{i+1}
Sb_{4x}^i	$(0,\pi(0))$	$(1,\pi(1))$	$(2,\pi(2))$	$(3,\pi(3))$
Sb_{4x+1}^i	$(1,\pi(1))$	$(2,\pi(2))$	$(3,\pi(3))$	$(0,\pi(0))$
Sb_{4x+2}^i	$(2,\pi(2))$	$(3,\pi(3))$	$(0,\pi(0))$	$(1,\pi(1))$
Sb_{4x+3}^i	$(3,\pi(3))$	$(0,\pi(0))$	$(1,\pi(1))$	$(2,\pi(2))$

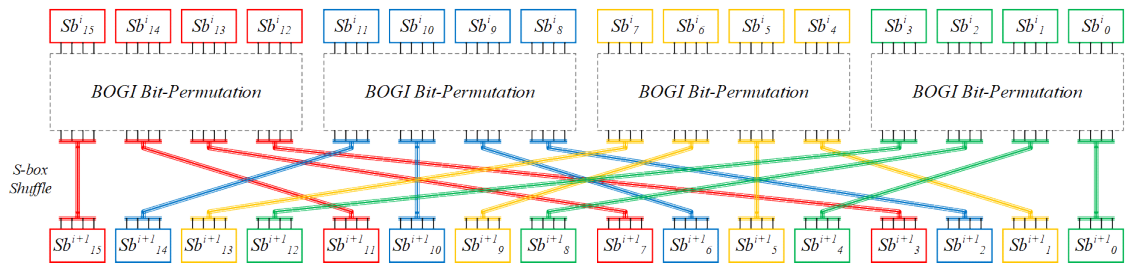

Fig. 7. GIFT 64-bit permutation

Table 6. Distribution of number of bit permutation

Number of Invariant Factors / π	8	10	12	14	16	18	20	22
π_1	-	-	-	-	408	72	72	24
π_2	-	24	300	108	48	72	12	12
π_3	-	24	300	108	48	72	12	12
π_4	288	96	72	24	72	24	-	-

이 필요함을 알 수 있다.

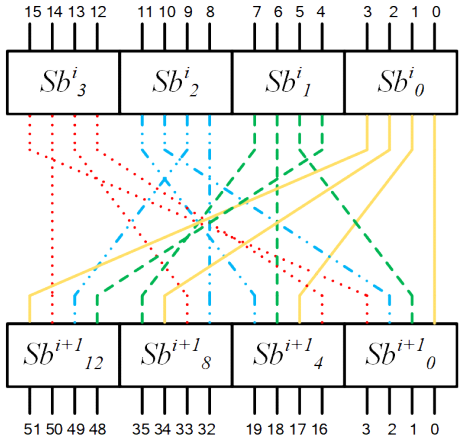

Fig. 8. Group mapping from $Q0$ to $R0$ in GIFT

V. 결 론

본 논문에서는 경량 블록암호의 선형계층이 비트 순열일 경우, 설계자 관점에서 라운드 키 간의 차분의 종류가 한가지여도 비선형 불변 공격에 저항성을 갖는 비트 순열의 형태와 개수를 도출하였다. 그리고 비트 순열의 경우, 불변 성분을 구하지 않고도 비트 순열을 구성하는 사이클의 개수와 위수를 통해 비선형 불변 공격에 대한 저항성을 측정할 수 있음을 보였다. 또한, PRESENT 구조 블록암호의 경우 비선형 불변 공격에 저항성을 가지려면 적어도 두 종류의 라운드 키 간의 차분이 필요함을 전수조사를 통해 확인하고, 두 종류의 라운드 키 간의 차분을 필요로 하는 비트 순열로 변경하여 탐색한 결과 PRESENT보다 적은 라운드와 적은 라운드 키 간의 차분의 종류를 이용하여 차분 공격과 비선형 불변 공격에 저항성을 보일 수 있었다. 마지막으로 GIFT의 S-box를 사용하면서 BOGI 설계 논리를 유지하는 모든 비트 순열의 불변 성분 분포를 통해, 변형된 GIFT 구조 블록암호는 비선형 불변 공격에 저항성을 갖기 위해 적어도 8종류의 라운드 키 간의 차분이 필요함을 보였다.

향후에는 GIFT 구조 블록암호에서 BOGI 설계 논리를 유지하는 모든 비트 순열에 대한 차분 공격, 선형 공격의 저항성을 연구할 수 있을 것이다. 또한, 일반적인 선형계층에서 비선형 불변 공격에 저항성을 갖는 최적의 선형계층의 형태와 개수의 도출 방안을 연구할 수 있을 것이다.

References

[1] TODO, Yosuke; LEANDER, Gregor; SASAKI, Yu. Nonlinear invariant attack. In: International Conference on the Theory and Application of Cryptology and Information Security. Springer, Berlin, Heidelberg, 2016. p. 3-33.

[2] BEIERLE, Christof, et al. Proving resistance against invariant attacks: How to choose the round constants. In: Annual International Cryptology Conference. Springer, Cham, 2017. p. 647-678.

[3] DUMMIT, David Steven; FOOTE, Richard M. Abstract algebra. Hoboken: Wiley, 2004.

[4] WEI, Yongzhuang, et al. Generalized nonlinear invariant attack and a new

design criterion for round constants. IACR Transactions on Symmetric Cryptology, 2018, 62-79.
〔5〕 LEANDER, Gregor, et al. A cryptanalysis of PRINTcipher: the invariant subspace attack. In: Annual Cryptology Conference. Springer, Berlin, Heidelberg, 2011. p. 206-221.
〔6〕 BEYNE, Tim. Block cipher invariants as eigenvectors of correlation matrices. Journal of Cryptology, 2020, 1-28.
〔7〕 CARLET, Claude; CRAMA, Yves; HAMMER, Peter L. Boolean functions for cryptography and error correcting codes. Boolean models and methods in mathematics, computer science, and engineering, 2010, 2: 257-397.
〔8〕 BOGDANOV, Andrey, et al. PRESENT: An ultra-lightweight block cipher. In: International Workshop on Cryptographic Hardware and Embedded Systems. Springer, Berlin, Heidelberg, 2007. p. 450-466.
〔9〕 BANIK, Subhadeep, et al. GIFT: a small present. In: International Conference on Cryptographic Hardware and Embedded Systems. Springer, Cham, 2017. p. 321-345.
〔10〕 BIHAM, Eli; SHAMIR, Adi. Differential cryptanalysis of DES-like cryptosystems. Journal of CRYPTOLOGY, 1991, 4.1: 3-72.
〔11〕 MATSUI, Mitsuru. Linear cryptanalysis method for DES cipher. In: Workshop on the Theory and Application of Cryptographic Techniques. Springer, Berlin, Heidelberg, 1993. p. 386-397.

〈저자소개〉

정 건 상 (Keonsang Jeong) 학생회원
2019년 2월: 고려대학교 수학과 졸업
2019년 3월~현재: 고려대학교 정보보호대학원 석사과정
〈관심분야〉 암호 알고리즘 설계 및 분석, 대칭키 암호

김 성 겸 (Seonggyeom Kim) 학생회원
2016년 8월: 한양대학교 수학과 졸업
2016년 9월~2018년 8월: 고려대학교 정보보호대학원 석사
2019년 3월~현재: 고려대학교 정보보호대학원 박사과정
〈관심분야〉 암호 알고리즘 설계 및 분석, 대칭키 암호, 난수발생기

홍 득 조 (Deukjo Hong) 종신회원
1999년 8월: 고려대학교 수학과 학사
2001년 8월: 고려대학교 수학과 석사
2006년 2월: 고려대학교 정보보호대학원 박사
2006년 3월~2007년 12월: 고려대학교 정보보호기술연구센터 연구교수
2007년 12월~2015년 8월: 국가보안기술연구소 선임연구원
2015년 9월~현재: 전북대학교 IT정보공학과 부교수
〈관심분야〉 암호 알고리즘 설계 및 분석

성 재 철 (Jaechul Sung) 종신회원
1997년 8월: 고려대학교 수학과 학사
1999년 8월: 고려대학교 수학과 석사
2002년 8월: 고려대학교 수학과 박사
2002년 8월~2004년 1월: 한국정보보호진흥원 선임연구원
2004년 2월~현재: 서울시립대학교 수학과 전임강사, 조교수, 부교수, 교수
〈관심분야〉 암호 알고리즘 설계 및 분석

홍 석 희 (Seokhie Hong) 종신회원
1995년: 고려대학교 수학과 학사
1997년: 고려대학교 수학과 석사
2001년: 고려대학교 수학과 박사
1999년 8월~2004년 2월: ㈜시큐리티 테크놀로지 선임연구원
2003년 3월~2004년 2월: 고려대학교 정보보호기술연구센터 선임연구원
2004년 4월~2005년 2월: K.U. Leuven ESAT/SCD-COSIC 박사후 연구원
2005년 3월~2013년 8월: 고려대학교 정보보호대학원 부교수
2013년 9월~현재: 고려대학교 정보보호대학원 정교수
〈관심분야〉 대칭키 및 공개키 암호 알고리즘, 부채널 공격 및 대응기법, 디지털 포렌식