논문 2011-48CI-2-13

# RSA-CRT의 향상된 등간격 선택 평문 전력 분석

## ( Enhanced Equidistant Chosen Message Power Analysis of RSA-CRT Algorithm )

박 종 연*, 한 동 국**, 이 옥 연***, 최 두 호****

( Jong-Yeon Park, Dong-Guk Han, Okyeon Yi, and Dooho Choi )

요 약

RSA-CRT알고리즘은 RSA알고리즘의 성능 향상을 위해 널리 쓰이고 있다. 하지만 일반적인 RSA 알고리즘처럼 CRT 버전의 RSA 또한 부채널 분석에 취약함이 알려져 왔다. 그 중 Boer등이 제안한 전력 분석 방법은 등간격 선택 전력 평문을 이용하여 CRT 알고리즘의 reduction단계를 분석하는 방법으로, 등간격 선택 평문 전력 분석 방법(Equidistant Chosen Messages Power Analysis, ECMPA)또는 MRED(Modular reduction on Equidistant data)분석 방법으로 알려져 있다. 이 방법은 등간격 선택 평문을 이용하여 입력 평문과 동일한 간격을 가지는 reduction 결과 값, $r = x \bmod p$ 을 찾는 방법으로, $r$의 노출에 의해 RSA의 비밀 소수 $p$가 계산 될 수 있다. 본 논문에서의 실험 결과, 이론 적으로만 알려져 있던 reduction 단계의 분석 결과가 기존 논문의 예상과는 다른 결과를 가짐을 확인하였다. 본 논문에서는 선택 bit에 의존한 Ghost key의 패턴과, reduction 알고리즘의 연산 과정에서 발생하는 Ghost key가 존재함을 이론적 및 실험적으로 증명하였다. 따라서 본 논문은 기존에 알려지지 않은 Ghost key의 특징에 대하여 논하며, 향상되고, 구체적인 공격 방법을 제안한다.

**Abstract**

RSA-CRT algorithm is widely used to improve the performance of RSA algorithm. However, it is also vulnerable to side channel attacks like as general RSA. One of the power attacks on RSA-CRT, proposed by Boer et al.[5], is a power analysis which utilizes reduction steps of RSA-CRT algorithm with equidistant chosen messages, called as ECMPA(Equidistant Chosen Messages Power Analysis) or MRED(Modular Reduction on Equidistant Data) analysis. This method is to find reduction output value $r = x \bmod p$ which has the same equidistant patterns as equidistant messages. One can easily compute secret prime $p$ from exposure of $r$. However, the result of analysis from a reduction step in [5] is remarkably different in our experiment from what Boer expected in [5]. Especially, we found that there are Ghost key patterns depending on the selection of attack bits and selected reduction algorithms. Thus, in this paper we propose several Ghost key patterns unknown to us until now, then we suggest enhanced and detailed analyzing methods.

**Keywords :** Side Channel Attacks, RSA-CRT, MRED, ECMPA, CPA

* 학생회원, 국민대학교 수학과
(Department of Mathematics, Kookmin University)
** 정회원, *** 정회원-교신저자, 국민대학교 수학과
(Department of Mathematics, Kookmin University)
**** 정회원, 한국전자통신연구원
(Electronics and Telecommunication Research Institute, ETRI)
※ 이 논문은 2010년도 정부(교육과학기술부)의 재원으로 한국연구재단의 기초연구사업 지원을 받아 수행된 것임 (20100024870)
※ 본 연구는 방송통신위원회 및 한국방송통신전파진흥원의 방송통신기술개발사업의 일환인 SCARF 프로젝트로 수행하였음. [부채널 공격 방지 원천기술 및 안전성 검증기술 개발]
접수일자: 2010년11월1일, 수정완료일: 2011년3월4일

## Ⅰ. 서 론

최근 스마트카드(Smart Card), 스마트 폰(Smart phone), 전자 여권 등의 사용이 일반화됨에 따라 부채널 분석 방법에 대한 안전성 문제가 대두되고 있다. 부채널 분석(Side Channel Analysis, SCA)은 기존의 암호 분석방법이 아닌, 알고리즘 구현 장비(Embedded device)의 전자파, 전력 등의 물리적인 특성들을 분석하여 알고리즘의 비밀 정보를 찾아내는 방법이다[1]. 그 중 소비되는 전력을 분석하는 방법(Power Analysis)은 단순전력분석(Simple Power Analysis, SPA), 차분전력분석(Differential Power Analysis, DPA)방법, 상관전력분석(Correlation Power Analysis, CPA)방법 등으로 발전되었으며, 부채널 분석 방법 중 가장 강력한 방법들 중 하나이다[2~3].

RSA 알고리즘에 대한 부채널 분석은 Messerges 등에 의해 제시된 SEMD(Single Exponent Multiple Data), MESD(Multiple Exponent Single Data), ZEMD(Zero Exponent Multiple Data)의 세 가지 방법이 있으며, 모두 공격자가 선택한 평문이 비밀 지수를 이용하여 지수 승이 연산되는 구간을 공격하는 방법이다[4].

CRT(Chinese Remainder Theorem)를 이용한 RSA 알고리즘은 지수의 길이와 밑수의 크기를 줄임으로써 동일한 구현 방법으로 알고리즘의 연산속도를 약 4배 정도 향상시키기 때문에 널리 사용되고 있으며, 비밀 소수를 이용하여 초기 reduction을 시행하여 일반적인 RSA 알고리즘에서의 메시지 보다 축소된 reduction결과 값과 지수 값으로 지수 승 연산을 시행하게 된다. 또한 비밀 소수를 알 수 없다는 한계점 때문에 중간 연산 값을 계산 해낼 수 없으며 기존의 ZEMD등의 부채널 분석 방법으로는 공격이 불가능 하다. 하지만 RSA-CRT 알고리즘은 초기 reduction단계와 재조합 단계가 반드시 필요하다는 특징이 있어 오히려 전력 분석에 대해 약점을 들어내며, 일반적인 DPA 분석 방법에서 탈피한 여러 가지 부채널 분석 방법이 제안 되었다. reduction단계를 분석하는 DPA방법으로는 Boer등이 제안한 등간격의 평문을 이용한 MRED(Modular Reduction on Equidistant Data)분석 방법이 알려져 있으며, 등간격의 선택 평문과 선 계산 값을 이용하여 DPA 또는 CPA를 수행하게 된다[5]. 이러한 분석의 특징 때문에, 등간격 선택 평문 전력 분석 방법(Equidistant Chosen Message Power Analysis, ECMPA)으로도 알려져 있다[12]. CRT-재조합 단계를 분석하는 방법으로는 DPA기반의 Amiel 등의 방법과, SPA 기반의 Novak의 방법이 알려져 있으며, Garner의 CRT알고리즘에서의 취약점을 분석 하였다[6~7].

전력 분석은 전력 모델에 의한 분석자의 계산 값과, 실제 전력 파형 간의 상관성이 존재하기 때문에 가능하다. 하지만 키 값이 틀림에도 불구하고 키와 유사한 형태로 계산이 되는 유사키의 형태는 전력 분석의 성능을 저하시키는 주요한 요인 중 하나이다. 이런 형태의 키는 일반적으로 Ghost key 또는 Ghost peak라는 용어로 쓰인다[3]. Ghost key의 패턴에 대한 사전 지식은 분석 결과를 해석함에 있어서 더 많은 정보를 제공 해 줄 수 있으며, 더욱 향상된 분석 시나리오를 도출해 내는 것에 이용 될 수 있기 때문에 그 자체로 충분한 의미가 있다. 특히, ECMPA 분석 방법은 난수 성을 가지는 기존의 분석 중간 값 연산과는 달리 일정한 규칙을 가지는 중간 값 연산을 이용하기 때문에, 더욱 다양한 Ghost key의 패턴이 나타난다.

본 논문은 reduction 단계의 공격인 ECMPA를 시뮬레이션이 아닌 실제 MCU chip의 소프트웨어 구현 환경에서 RSA-CRT reduction 알고리즘을 활용 한 분석 결과를 바탕으로 상관 전력 분석에서의 Ghost key에 일반적으로 고려되는 패턴과는 다르게 나타나는 특징에 대하여 논한다. 특히, 분석 선택 bit에 의존하여 발생할 수 있는 Ghost key의 성질과[12], reduction 알고리즘에 의존하여 나타나는 Ghost key의 성질에 대해 밝히고, 그 성질을 바탕으로 분석 위치까지 고려한 ECMPA 방법을 제안한다.

본 논문은 다음과 같이 구성된다. Ⅱ장에서는 본 논문에 사용되는 기호들과 알아두어야 할 사전지식에 대한 내용을 다룰 것이며, Ⅲ장에서는 선택 bit에 의존한 Ghost key의 패턴에 대하여 설명하며, Ⅳ장에서는 reduction 알고리즘 연산 단계에서 발생하는 Ghost key의 특징에 대한 분석과, Ⅴ장에서는 Ⅳ장에서 논한 Ghost key의 의미와 적용을 설명하며, 마지막으로 Ⅵ장에서는 본 논문을 결론짓는다.

## Ⅱ. 사전 지식과 기호들

### 1. 기호 및 용어

- $N$ : 전력 파형의 개수 (또는 입력 평문의 개수)

- $K$ : 추측키 전체의 개수
- $R$ : 분석 bit 크기
- $HW(v)$ : $\sum_{i=0}^{R-1} b_i$, $v$의 헤밍웨이트 (단, $v$는 하나의 이진 값 $(b_{R-1}b_{R-2}...b_0)_2$)
- $\{v_{i,j}\}=\{f(d_i,k_j)\}$ $(i=0,...,N-1\ ,\ j=0,...,K-1)$ : $j$번째 추측키 $k_j$와 $i$번째 평문정보 $d_i$에 해당하는 추측키에 의한 선 계산 값 집합 .
- $f$ : 분석 알고리즘과 공격 지점에 의존 한 중간 값 계산 함수. 일반적인 블록 암호의 경우 Look up table 출력 등이 쓰일 수 있음.
- $\{key\} = \{k_j \mid 0 \le j \le K-1\}$ : 키 후보 전체 집합
- $C = \{b_i \mid i \in S,\ S \subseteq \{0,1...R-1\}\}$ ($S$는 선택 bit위치 집합, $C$는 선택 bit 집합)
- $v_{\max order}$ : $\max(S)$ 집합 $S$의 원소 중 최댓값
- $v_{\min order}$ : $\min(S)$ 집합 $S$의 원소 중 최솟값
- $HW_{chosen}(v,C)=\sum_{b_i \in C} b_i$
- $\{h_{i,j}\}=\{HW_{chosen}(v_{i,j},C) \mid 0 \le i \le N-1\ , 0 \le j \le K-1\}$
- $\{v_k\}=\{v_{i,k} \mid 0 \le i \le N-1,\ k$ 는고정된$key\}$ : 고정된 하나의 key에 선 계산 값 집합
- $\{h_k\}=\{h_{i,k} \mid 0 \le i \le N-1,\ k$ 는고정된$key\}$ : 고정된 하나의 key에 대한 선택 bit의 선 계산 값 집합.
- Ghost Key : 높은 상관계수 값을 갖는 틀린 키 값
- $MSB_g(v)$ : $v \bmod 2^g$, $\{b_i \mid R-g \le i \le R-1\}$, 상위 $g$개의 bit.
- $LSB_g(v)$ : $\lfloor x/2^{R-g} \rfloor$, $\{b_i \mid 0 \le i \le g-1\}$, 하위 $g$ 개의 bit.

## 2. RSA알고리즘과 RSA-CRT알고리즘

RSA알고리즘은 가장 널리 쓰이는 공개키 암호 중 하나로, 두 소수의 곱 $p \times q$은 알더라도, $p$와 $q$값을 알아내는 문제의 난해성을 기반으로 한다[8]. 암호화 된 메시지 $C$에 대하여, 비밀 지수 $d$을 이용한 지수 승 연산 $M = C^d \bmod (p \times q)$을 통하여 평문 $M$을 복호화 하는 연산은 RSA알고리즘의 연산 중 가장 큰 시간 소비를 차지하는 부분이며, 중국인의 나머지 정리(Chinese Remainder Theorem, CRT)를 이용하여 지수와 밑수의 크기를 반으로 줄여, 알고리즘의 연산시간을 향상 시킨다[9]. RSA-CRT는 다음의 두 단계의 연산으로 RSA의 $M = C^d \bmod (p \times q)$ 연산과 동일한 연산 결과 값을 가져 올 수 있다. $d_p = d \bmod (p-1)$, $d_q = d \bmod (q-1)$에 대하여,

단계 1(지수 승) : $C_p = C^{d_p} \bmod p,\ C_q = C^{d_q} \bmod q$

단계 2(재조합) : $M_0 = (C_q - C_p) \times p^{-1} \bmod q$

$$M = C_p + M_0 \times p$$

단계 1의 지수 승 연산은 최초 $r = C \bmod p$ 연산이 포함되며, 이 연산을 본 논문은 초기 reduction연산 이라고 부르기로 한다. 위 과정을 이용하여 효율적인 지수 승 연산을 수행하며 CRT를 사용하지 않은 RSA 알고리즘과 동일한 출력 값을 갖는다.

## 3. 등간격 선택 평문 전력 분석 방법

2002년 Boer 등은 RSA-CRT 알고리즘의 DPA 공격 기법인 MRED 분석기법을 발표하였다[5]. MRED 분석은 RSA-CRT 알고리즘의 초기 reduction과 재조합 단계 중 reduction 단계의 취약점을 분석하는 방법이다. 이 공격은 입력 메시지 $x$와 $x \bmod p = r$에 대하여 $i \le p$일 때, 수식(1)이 성립하기 때문에 소수 $p$를 모르더라도 직접적으로 $r$의 최하위 Byte 값을 추정 할 수 있다.

$$x - i \bmod p = r - i \tag{1}$$

이때, $r$을 추정하기 위한 중간 값 집합은 $\{v_{i,j}\}=\{v_{i,j} \mid (j-i) \bmod 256,\ i=0,...,N-1, j=0,...,K-1\}$로 계산 된다. 이때에, 공격자는 선택 bit를 반영한$\{h_{i,j}\}$를 계산하여 CPA 또는 DPA 공격을 할 수 있다. 공격자는 최하위 byte 공격을 통해 $r$의 최하위 byte를 계산하는 것과 동일한 기법으로 상위 byte를 공격 할 수 있다.

$$x - i(256)^s \bmod p = r - i(256)^s \tag{2}$$

(단, $i(256)^s \le p$ 이며, $s$는 최하위 byte로 부터의 byte 순서, $s$는 0일 때 최하위 byte 공격 이다.) 식(2) 은 식(1)을 최하위 byte로 부터 상위 $s$+1번째 byte로 확장 시킨 것이며, 상위 byte역시 $\{v_{i,j}\}$과 동일한 중간 값 집합 을 이용하여 공격 할 수 있다. 식(2)은 $r \ge i(256)^s$이 만족되면 성립하기 때문에, 공격자는 평문의 개수만큼 $i$값을 변화 시켜서 $r$의 값을 추측을 할 수 있으며, $r$값을 찾으면 $N=pq$ 일 때, $GCD(x-r,N)=p$임을 이용하여 $p$을 계산할 수 있다.

## Ⅲ. 선택 bit에 의존한 Ghost key의 패턴

DPA 또는 CPA 분석 시 식(2)에 의해 ECMPA 공격을 위한 중간 값 계산을 한 뒤, 분석을 위한 선택 bit위치를 결정하여 $S$를 구성한다. $S$는 ${}_RC_1+{}_RC_2+{}_RC_3+...+{}_RC_R=2^R-1$개의 선택 경우에 따라서 구성이 가능하다. 선택bit가 정해지면 $\{h_{i,j}\}$를 계산할 수 있다. 본 절에서는 선택 bit에 의존하여 발생하는 Ghost key의 패턴은 최상위 선택 bit와 최하위 선택 bit에 의존하여 나타남을 보인다. 본 논문에서 사용되는 용어 key는 ECMPA 분석 결과 값인 $r$과 혼용되어 사용 될 것이다.

### 1. 선택 최상위 bit에 의존한 Ghost key 패턴

**정의 1(수열 적으로 같은 집합)**

$A=\{a_0,a_1,...,a_{N-1}\}$, $B=\{b_0,b_1,...b_{N-1}\}$ 에 대하여 $a_0=b_0,\ a_1=b_1,\ \cdots,\ a_{N-1}=b_{N-1}$ 이 성립하면, 집합 A와 B는 수열 적으로 같은 집합이며, A ≒ B 로 표기한다.

중간 값 집합 A, B에 대하여 A와 B가 수열 적으로 같은 집합이면, CPA 분석 시 계산되는 상관계수가 일치 할 것이다. 다음의 정리는 선택 최상위 bit에 의존하여 나타나는 Ghost key의 패턴의 일반적 성질을 보여준다.

**정리 1 (동일 키 존재성)**

$n=v_{\max order}+1$, $\forall k\in\{key\}$에 대하여 $\{h_k\}\doteq\{h_{k+2^n \bmod 2^R}\}$이 성립한다.

증명) $x_1,x_2\in Z$, $x_1=x_2+2^n$ 라고 하자. $x_1$과 $x_2$의 $LSB_n$에 대하여, $x_1 \bmod 2^n=x_2+2^n \bmod 2^n=x_2 \bmod 2^n$ 이 성립하므로 $LSB_n(x_1)=LSB_n(x_2)$ 이다. $n$이 최상위 bit 위치 값(max bit order) + 1이므로 $\{h_k\}$는 $\{v_k\}$의 $LSB_n$이며, 정의에 의해 $\{h_k\}\doteq\{h_{k+2^n \bmod 2^R}\}$이 성립한다. □

그림 1과 그림 2는 $R$=8 에서 256개의 키 후보에 대한 $LSB_4$와 $LSB_6$ 선택비트의 CPA의 분석의 최대 상관계수 값이다. 그림 1 의 경우 임의의 키 $k$의 중간 값 집합과 $k+2^4 \bmod 256$의 중간 값 집합은 수열 적으로 같은 집합이다. 따라서 16을 주기로 같은 중간 값을 가지

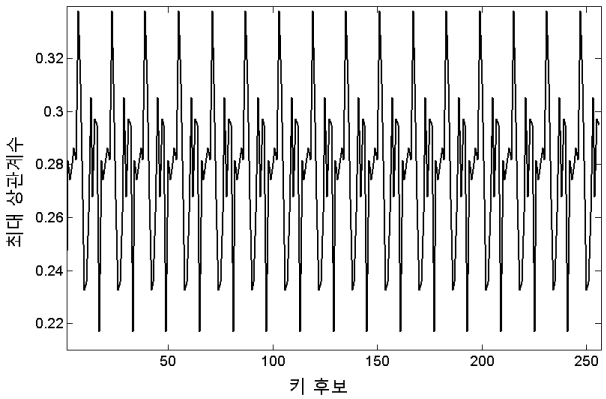


그림 1. $LSB_4$ 분석, CPA 키 후보에 대한 분석 구간에서의 최대 상관계수

Fig. 1. Maximum correlation coefficient values of key candidates on $LSB_4$.

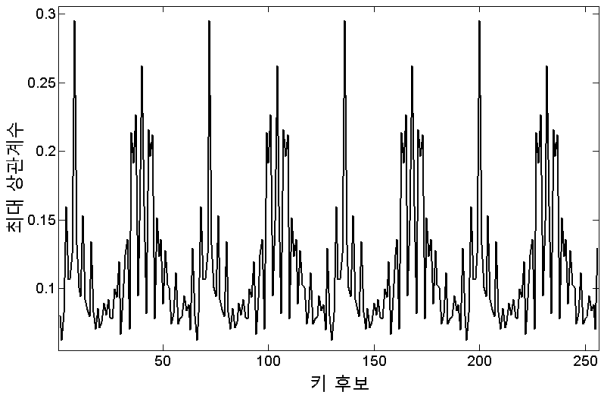


그림 2. $LSB_6$ 분석, CPA 키 후보에 대한 분석 구간에서의 최대 상관계수

Fig. 2. Maximum correlation coefficient values of key candidates on $LSB_6$.

며, 256개의 키 후보에 대하여 16(=256/16)개의 키 후보가 존재하게 된다. 따라서 선택 최상위 bit에 의존하여 존재할 수 있는 Ghost key는 주기적인 키 패턴의 특징을 가지고 있음을 알 수 있으며, 공격 중간 값이 수열 적으로 같기 때문에 생기는 현상이다.

### 2. 선택 최하위 bit에 의존한 Ghost key 패턴

최상위 선택 bit뿐만 아니라 최하위 선택 bit역시 Ghost key의 패턴을 가지고 있다. 다음의 정리는 최하위 bit에 의존하여 나타나는 Ghost key의 패턴의 일반화된 형태를 보여준다.

**예비정리 1**

임의의 $x,m\in Z$에 대하여,

$\lfloor x/2^m \rfloor \neq \lfloor (x-1)/2^m \rfloor \iff x \bmod 2^m=0$ 이다.

**정리 2 (주변 키 유사성)**

$m = v_{\min order}$, 임의의 $k \in \{key\}$ 에 대하여, $\{h_k\}$의 원소 $N$개 중 $\left\lfloor N \times \frac{1}{2^m} \right\rfloor$ 개의 원소를 제외하면 $\{h_k\} \doteq \{h_{k+1}\}$ 가 성립한다.

증명) $\{v_k\} = \{x_1, x_2, ...x_N\}$, $\{v_{k+1}\} = \{x_0, x_1, ...x_{N-1}\}$ 라 두면, $\forall x_i \in \{v_k\}$ 에 대하여 $x_i - 1 = x_{i+1}$ 이다. $MSB_{R-m}(x)$에 대하여, 예비정리 1에 의해 모든 $x_i \in \{v_k\}$에 대하여 $h_i = HW(\lfloor x_i / 2^m \rfloor)$이 만족되는 두 개의 집합 $\{h_k\} = \{h_0, h_1, ...h_{N-1}\}$, $\{h_{k+1}\} = \{h_1, h_2, ...h_N\}$을 생각해 볼 수 있다. $x_i - 1 = x_{i+1}$인 성질과, 예비정리 1에 의해, $\{h_k\} = \{h_0, h_1, ...h_{N-1}\}$는 $\{h_{k+1}\} = \{h_1, h_2, ...h_N\}$과 오직 $x \bmod 2^m = 0$ 일 때에만 다른 값을 가지므로, 두 집합은 오직 $N \times \frac{1}{2^m}$ 개의 수열 적으로 다른 원소를 갖는다. 한편 $N$은 $2^m$에 의해 항상 나누어지지 않으므로, 집합 $\{h_k\} = \{h_0, h_1, ...h_{N-1}\}$과 $\{h_{k+1}\} = \{h_1, h_2, ...h_N\}$는 정확히 오직 $\left\lfloor N \times \frac{1}{2^m} \right\rfloor$ 개의 수열 적으로 다른 원소를 갖는다. 그러므로 $N$개의 원소 중 $\left\lfloor N \times \frac{1}{2^m} \right\rfloor$ 개의 원소를 제외하면 $\{h_k\} \doteq \{h_{k+1}\}$가 성립한다. □

최하위 선택 bit에 의존해서는 선택 최상위의 주기적 성질이 나타나지 않는 반면, 주변키와의 유사적 특징이 나타난다. 이 유사성은 key와 key+1 사이 계산된 중간

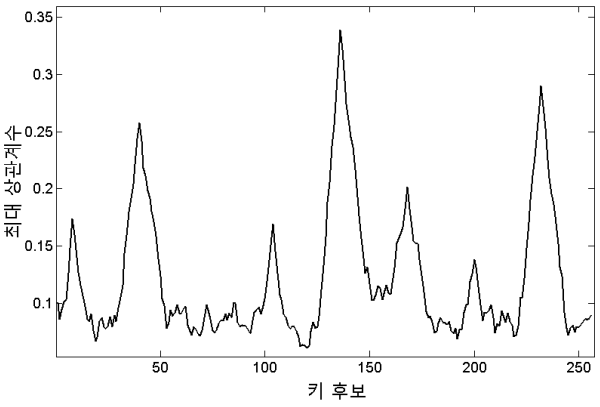


그림 3. $MSB_4$ 분석, CPA키 후보에 대한 분석 구간에서의 최대 상관계수

Fig 3. Maximum correlation coefficient values of key candidates on $MSB_4$.

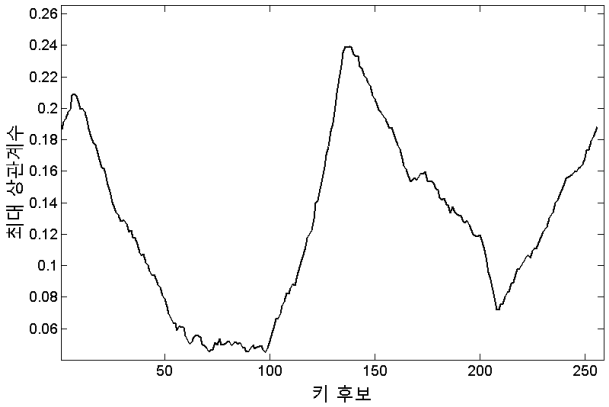


그림 4. $MSB_1$ 분석, CPA키 후보에 대한 분석 구간에서의 최대 상관계수

Fig. 4. Maximum correlation coefficient values of key candidates on $MSB_1$.

값 집합의 일정 비율의 유사성이다. 그림 3과 그림 4는 최상위 4bit와 최상위 1bit의 CPA 분석에서의 전체 키 후보에 대한 최대 상관 계수를 나타낸 것이다. 정리 2에 의하여 최상위 4bit 분석은 15/16의 비율로 같은 중간 값을 가지며, 최상위 1bit 분석은 127/128의 비율로 같은 중간 값을 가진다. 또한 key+1과 key+2 사이의 유사성도 존재 하므로, key 주변의 key+$\alpha$($\alpha \in Z$) 에 대해 일반적으로 유사성이 존재한다고 볼 수 있으며, 전반적으로 부드러운 곡선 모양의 상관계수 형태를 나타낼 것이다. 최상위 4bit 분석보다 최상위 1bit 분석이 비율 적으로 유사한 중간 값을 가지므로, 더 부드러운 최대 상관계수 곡선이 나타난다.

그림 5와 그림 6은 최상위 1bit 분석 시 key와 Ghost key의 공격 구간 전체 point에 대하여 상관계수를 그림

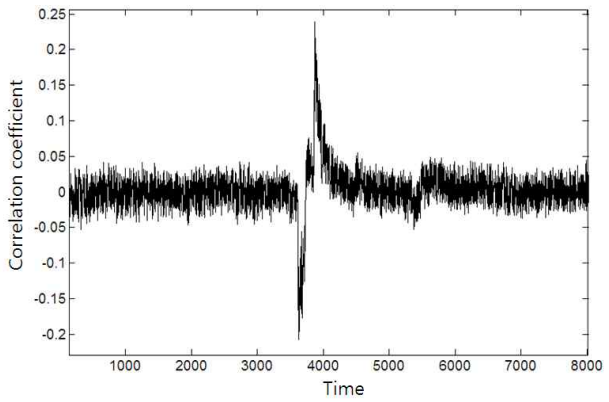


그림 5. $R$=8, key(0x69)의 저장구간에서의 $MSB_1$의 CPA 분석 상관계수

Fig. 5. $R$=8, Correlation coefficient in saving time on $MSB_1$ of key(0x69).

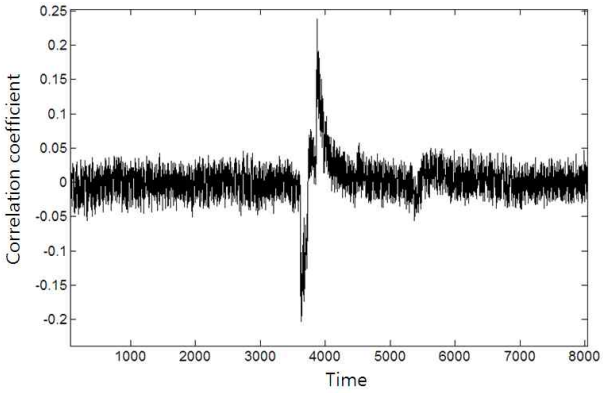


그림 6. $R$=8, key(0x6A)의 저장구간에서의 $MSB_1$의 CPA 분석 상관계수

Fig. 6. $R$=8, Correlation coefficient in saving time on $MSB_1$ of key(0x6A).

으로 나타낸 것이다. 중간 값이 127/128의 비율로 같기 때문에 상관계수 역시 전체적으로 동일한 형태를 나타냄을 알 수 있다.

### 3. 선택 bit에 의존하지 않은 일반적인 Ghost key

최상위 또는 최하위에 대한 선택이 없이 전체 레지스터 크기를 분석을 했을 때에도 Ghost key가 존재한다. 이 장에서 논할 Ghost key는 기존의 Boer 에서 전체키의 중간 값 집합에 대한 상관계수를 계산하여 언급한 바 있다[5]. 본 논문에서는 단순 계산으로 보여주는 것이 아닌 다음의 일반화된 정리를 통해 Ghost key의 패턴을 나타낼 것이다.

**정리 3(일반적인 Ghost key의 패턴)**

임의의 $x \in Z_{2^R}$ 와 $w \in \{1,2...,R\}$에 대하여,

$\max(|HW(x \pm 2^w \bmod 2^R) - HW(x)|) = R - w$ 이다.

증명) $x \in Z_{2^R}$ , $y = x + 2^w \bmod 2^R$ 라 두자. division 알고리즘에 의해 $x$, $y$는 $x = 2^w \lfloor x/2^w \rfloor + x \bmod 2^w$,

$y = (2^w \lfloor x/2^w \rfloor + x \bmod 2^w + 2^w) \bmod 2^R$

$= (2^w(\lfloor x/2^w \rfloor + 1) + x \bmod 2^w) \bmod 2^R$ 로 표현할 수 있다. $x$와 $y$의 $LSB_w$ bit 만 고려한다면, 예비정리1에 의해,

$$HW(x \bmod 2^w) = HW((2^w \lfloor x/2^w \rfloor + x \bmod 2^w) \bmod 2^w)$$
$$= HW((2^w \lfloor x/2^w \rfloor \bmod 2^w) + x \bmod 2^w),$$
$$HW(y \bmod 2^w) = HW(((2^w \lfloor x/2^w \rfloor + 1) + x \bmod 2^w) \bmod 2^w)$$
$$= HW((2^w(\lfloor x/2^w \rfloor + 1) \bmod 2^w) + x \bmod 2^w)$$
$$= HW(x \bmod 2^w)$$

을 만족한다. 즉, $x$ 와 $y$ 는 $LSB_w$에 대해 같은 값을 갖는다. 따라서 $|HW(x \pm 2^w \bmod 2^R) - HW(x)|$ 는 기껏해야 $R-w$의 헤밍웨이트 차이 갖는다. □

정리 3에 의해 임의의 key와 key+$2^w$의 분석 결과 사이에는 일정 상관도가 늘 존재함을 알 수 있다. 예를 들어 $w$=7 이고 $R$=8이라고 할 때,

$$\{v_0\} = \{0,255,254,253,252,251...,0-N+1 (\bmod 256)\}$$
$$\{v_{128}\} = \{128,127,126,125,124,123...,127-N+1 (\bmod 256)\}$$
$$\{h_0\} = \{h_{0,0},h_{1,0},h_{2,0},h_{3,0}...\} = \{0,8,7,7,6,7...,\}$$
$$\{h_{128}\} = \{h_{0,128},h_{1,128},h_{2,128},h_{3,128},...\} = \{1,7,6,6,5,6...\}$$

이며, $\{h_0\}$와 $\{h_{128}\}$은 수열 적으로 같은 집합이 아니므로 주기적인 성질이 존재 하지 않고, 128은 0의 주변키에 속하지 않으므로, 정리 2에 의한 Ghost key패턴의 영향도 받지 않는다. 하지만 정리 3에 의해 두 집합 간의 헤밍웨이트가 기껏해야 1이 다르므로, 8bit 분석임에도 불구하고, 1bit의 CPA분석 차이 밖에 가져가지 못함을 알 수 있다. 그림 7은 8bit 분석 시 key(0x69)을 포함한 여덟 개 부분의 Ghost key 패턴을 볼 수 있다. 가운데 제일 높은 상관계수 값은 맞는 키 값에 대한 최대 상관계수 peak이며 가장 오른쪽 Ghost key는 0xE9(=0x69+27) 이다. 다른 높은 상관계수를 갖는 Ghost key 패턴은 정리 3 에서 $w$=5, $w$=6 일 때, 나타 날 수 있는 key$\pm 2^w \bmod 256$ 임을 그림을 통해 알 수 있다.

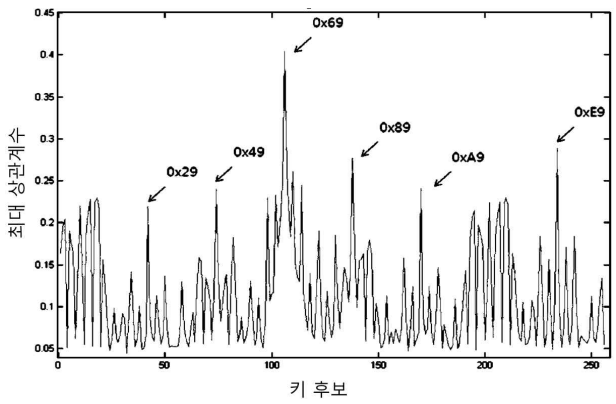


그림 7. 8bit 분석, CPA키 후보에 대한 분석 구간에서의 최대 상관계수

Fig. 7. Maximum correlation coefficient values of key candidates on 8bit.

## Ⅳ. 알고리즘에 의해 발생하는 Ghost key패턴

### 1. 뺄셈 단계에서 발생하는 Ghost key

ECMPA방법은 등간격의 평문이 등간격의 나머지를 만들어내는 산술적인 성질, 식 (2)를 이용한 것이다. 하지만 $x \bmod p = r$ 외에 다른 키에서 같은 등간격의 형태를 가지는 중간 값이 존재한다면, 이 키는 Ghost key가 될 것이다. 즉, 등간격의 선택 평문 $\{x, x-1, x-2, ..., x-N+1\}$에 대하여 $\{r, r-1, r-2, ..., r-N+1\}$역시 등간격을 만족 시킬 수밖에 없다는 것이 ECMPA의 분석 원리이며, 또 다른 등간격의 $\{u, u-1, u-2, ..., u-N+1\}$ 집합이 존재한다면 $u$역시 Ghost key가 된다. 집합의 원소를 약간 변형하여, Ghost key $u$의 존재와 같은 원리로, $u = r+c$를 만족시키는 상수 $c$가 존재한다고 했을 때, $\{r+c, r+c-1, r+c-2, ..., r+c-N+1\}$역시 등간격의 성질을 가지며, Ghost key가 된다.

그림 8과 그림 9는 key와 Ghost key의 뺄셈 연산과 reduction 결과의 저장 부분의 CPA 분석 결과이다. 뺄셈 연산부분은 Ghost key와 key 모두 높은 상관계수를 보여주며, 그림 8에서만 오른쪽 저장부분의 높은 상관계수 봉우리가 발생함을 볼 수 있다. 이것은 $r$값과 직접적인 연관이 없는 Ghost key가 저장 부분과 독립적인 연산에서 나타남을 알 수가 있으며, 정확한 시간적 위치는 reduction 연산의 마지막 뺄셈 연산이다. 그 이유는 몫 과 나머지를 계산하는 reduction 연산은 마지막 단계에서 몫에 의존하는 상수 또는 나누는 수를 이용하여 뺄셈 연산 $u - c = r$을 가지는 것이 일반적이기 때문이다. 따라서 Ghost key $u = r + c$가 반드시 존재하게 된다.

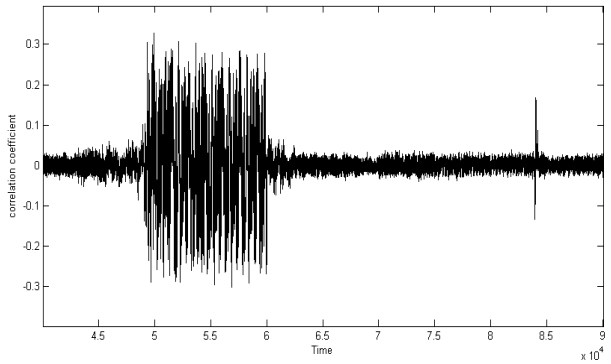


그림 8. key의 뺄셈과 저장 단계의 상관계수
Fig. 8. Correlation Coefficient on Subtraction and Saving step of Key.

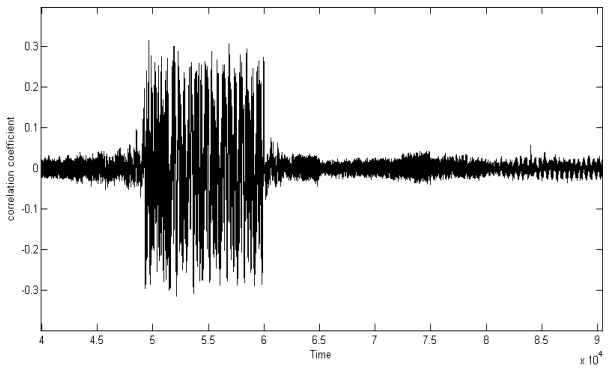


그림 9. Ghost key의 뺄셈과 저장 단계의 상관계수
Fig. 9. Correlation Coefficient on Subtraction and Saving step of Ghost Key.

그러므로 ECMPA방법은, reduction 알고리즘의 구현 방법과 뺄셈 연산에서의 상수 값에 의존한 Ghost key의 형태를 가진다.

그림 10과 그림 11은 reduction 알고리즘을 예로 나타낸 것이다. 그림 10은 $x \bmod p = r$ 의 연산의 예로써, $x \bmod p$=0x29C630 이며, 그림 11은 $x - 1 \bmod p$ =0x29C629로 $x$의 등간격이 $r$의 등간격으로 나타나는 것을 볼 수 있다. 하지만 마지막 뺄셈 연산단계의 0x245CFFA6과 0x245CFFA5 역시 등간격을 나타나며, 이 값은 ECMPA의 공격 가정에 따라서 Ghost key로 나타난다.

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | 05 | 5F | 2E | CE | |
| 2C FC 8D | | F1 | A8 | B3 | 11 | 55 | A6 | X |
| | - | E0 | EE | C1 | | | | |
| | | 10 | B9 | F2 | 11 | | | |
| | - | 10 | B1 | B8 | 53 | 55 | | |
| | | | 08 | 39 | BE | | | |
| | | - | 08 | 15 | 61 | 56 | | |
| | | | | 24 | 5C | FF | A6 | |
| | | | - | 24 | 33 | 39 | 76 | |
| | | | | | 29 | C6 | 30 | |

그림 10. $x \bmod p = r$ 연산
Fig 10. $x \bmod p = r$ operation.

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | 05 | 5F | 2E | CE | |
| 2C FC 8D | | F1 | A8 | B3 | 11 | 55 | A5 | X-1 |
| | - | E0 | EE | C1 | | | | |
| | | 10 | B9 | F2 | 11 | | | |
| | - | 10 | B1 | B8 | 53 | 55 | | |
| | | | 08 | 39 | BE | | | |
| | | - | 08 | 15 | 61 | 56 | | |
| | | | | 24 | 5C | FF | A5 | |
| | | | - | 24 | 33 | 39 | 76 | |
| | | | | | 29 | C6 | 29 | |

그림 11. $x - 1 \bmod p = r - 1$ 연산
Fig. 11. $x - 1 \bmod p = r - 1$ operation.

## V. 알고리즘에 의해 발생하는 Ghost key의 이용

### 1. Reduction 알고리즘

reduction알고리즘은 여러 가지가 알려져 있으나, 일반적으로 Barret reduction과 Montgomery reduction알고리즘이 사용된다[10~11]. Montgomery reduction의 경우 지수 승 연산에서 이용 시 성능을 극대화 시킬 수 있기 때문에 일반적으로 곱셈 알고리즘에 적용되어 사용된다. 하지만, Montgomery reduction은 RSA-CRT의 소수에 의한 초기 reduction연산으로 사용하기에는 비효율 적이며, CRT의 초기 reduction으로는 Barret reduction 알고리즘 등이 주로 사용된다. reduction 알고리즘은 일반적으로 블록 단위의 나눗셈, 그리고 곱셈, 덧셈, 뺄셈연산의 조합으로 이루어져 있으며, 뺄셈 단계에서 나타나는 Ghost key는 CRT의 reduction에서 반드시 나타나는 일반적인 패턴임을 알 수 있다.

### 2. Barrett Reduction의 뺄셈 단계에서 발생하는 Ghost key의 이용

알고리즘 1. barrett Reduction 알고리즘

$input$: $p, b \geq 3,\ k = \lfloor \log_b p \rfloor + 1,\ 0 \leq x \leq b^{2k}$, and $\mu = \lfloor b^{2k}/p \rfloor$

$output$: $x \bmod p$

$step\,1.\ \hat{q} = \lfloor \lfloor x/b^{k-1} \rfloor \times \mu / b^{k+1} \rfloor$

$step\,2: r = (x \bmod b^{k+1}) - (\hat{q}\, p \bmod b^{k+1})$

$step\,3$: $If\ r < 0\ then\ r = r + b^{k+1}$

$step\,4$: $While\ r \geq p\ do$: $r = r - p$

$step\,5: Return(r)$

알고리즘 1. Barrett Reduction을 보자, step 4에서 소수 $p$를 빼는 단계가 존재하며, $p$는 고정 값이므로 $p$는 4장에서 설명한 덧셈의 상수 $c$로 작용한다. 더욱이, 이 단계에서 나타나는 Ghost key는 $p$를 직접적으로 찾는 방법으로 이용 될 수도 있다. 공격자는 step 4의 마지막 단계에서 발생하는 두개의 key후보 들을 찾을 수 있으며, 두개의 key후보는 key인 $r$과 Ghost key $r+p$이다. 단순히 이 뺄셈 구간만을 공격 구간으로 선정한다면 공격자는 두개의 키 후보, $r$과 $r+p$, 중 어떤 값이 key인지 알 수가 없다. 그래서 공격자는 공격 구간 선택이 중요하다. 공격자에 의해 $r$과 $r+p$가 구분되어 분석됐다고 가정했을 때, $(r+p)-r=p$ 이므로 $p$를 직접 찾는 것이 가능하다.

### 3. 공격 구간 선택의 중요성

ECMPA 방법에서는 알고리즘에 의존하여 Ghost key가 발생하므로 공격 구간을 정확히 정하는 것이 중요하다. 공격 구간에 따라서 나타나는 상관계수의 패턴이 의미하는 결과가 달라지기 때문이다. key에 대하여 높은 상관계수를 나타내는 구간은 총 세 부분으로 나타날 수 있다.

첫째, reduction연산 구간 중, 뺄셈 연산이 나타나는 구간
둘째, reduction연산 결과가 저장되는 구간
셋째, reduction연산 결과를 RSA 지수 승 연산에 이용하는 데이터 불러오기 구간

첫 번째 구간은 뺄셈 구간에서 Ghost key가 발생하므로 높은 상관계수를 이용하여 키를 찾아내는 것이 쉽지 않다. 두 번째 구간은 공격이 가능하지만, 뺄셈 연산과 동시에 일어나며 데이터를 따로 저장하는 구간이 존재하지 않을 가능성이 있다. 따라서 세 번째 구간이 Ghost key로부터 영향을 받지 않는 공격 구간이 될 것이다. RSA-CRT의 초기 reduction은 두 개의 소수 $p$와 $q$에 대해서 연산되며, reduction 연산이 먼저 수행되는 소수 $p$를 추측할 때에 소수 $q$에 대한 reduction 연산까지 모두 마친 뒤, RSA 지수 승 연산을 위해 $r$을 불러올 때의 파형을 분석한다면 뺄셈 연산에 의한 Ghost key의 영향을 받지 않는다.

## VI. 결 론

본 논문에서는 ECMPA에서 선택 bit에 의한 Ghost key의 패턴과 알고리즘에 의존한 Ghost key의 패턴에 대하여 논하였다. 이 특징은 등간격의 평문을 사용하는 기법상의 특징 때문에 발생하는 것이며, MRED분석에서 필연 적으로 나타날 수 있는 특징이라는 것을 알았다. 선택 bit에 의존한 Ghost key의 특징은 연산 레지스터의 크기를 고려한 분석을 하는데 있어서 중요한 단서가 될 것이며, 향상된 DPA 또는 CPA분석 방법을 연구하는 데 중요한 결과가 될 것이다. 알고리즘에 의존한

Ghost key의 패턴은 분석의 시간적인 위치선정의 중요성을 보여주며, barrett reduction 알고리즘에서 $p$를 직접적으로 찾는 방법으로도 이용될 수 있다. 향후에는 여러 가지 Ghost key의 패턴에 대하여 더욱 일반화된 결과를 만들어 낼 것이며, 지금의 결과와 새로운 결과를 바탕으로 더욱 향상된 DPA분석 방법을 연구할 것이다.

## 참 고 문 헌


[1] P.Kocher, J.Jaffe, and B. Jun, “Introduction to differential power analysis and related attacks,” 1998, White Paper, Cryptography Research, http://www.cryptography.com/dpa/technical, 1998.

[2] P. Kocher, J. Jaffe, and B. Jun, “Differential power analysis,” Advances In Cryptology - CRYPTO′ 99, LNCS 1666 Springer-Verlag, pp. 388-397, Santa Barbara, USA, August 1999.

[3] E. Brier, C. Clavier, and F. Olivier, “Correlation power analysis with a leakage model,” Cryptographic Hardware and Embedded Systems 2004. LNCS 3156 Springer-Verlag, pp. 16-29, 2004.

[4] T.S.Messerges, E.A. Dabbish and R.H. Sloan, “Power Analysis Attacks of Modular Exponentiation in Smartcards”, Cryptographic Hardware and Embedded Systems 1999, LNCS 1717 Springer-Verlag, pp. 144-157, 1999.

[5] B. D. Boer, K. Lemke, and G. Wicke, “A DPA attack against the modular reduction within a crt implementation of RSA”, Cryptographic Hardware and Embedded Systems 2002, LNCS 2523 Springer-Verlag, pp. 228-243, 2002.

[6] Frederic Amiel, Benoit Feix, and Karine Villegas, “Power Analysis for Secret Recovering and Reverse Engineering of Public Key Algorithms”, International conference on Selected area in cryptography 2007, LNCS 4876 Springer-Verlag, pp 110-125, 2007.

[7] Roman Novak “SPA-Based Adaptive Chosen -Ciphertext Attack on RSA Implementation”, Public Key Crptography 2002, LNCS 2274 Springer-Verlag, pp. 252-262, 2002.

[8] Rivest R, Shamir A, Adleman L. “A method for obtaining digital signatures and public-key cryptosystems”, Communications of the ACM, vol 21, Issue 2, pp. 120-126, 1978.

[9] J. J. Quisquater and C. Couvreur, “Fast decipherment algorithm for RSA public key cryptosystem,” Electronic Letters, vol. 18, No 21, pp. 905-907, 1982.

[10] P. Barrett, “Implementing the Rivest Shamir and Adleman Public Key Encryption Algorithm on a Standard Digital Signal Processor” Advances In Cryptology - CRYPTO′ 86, LNCS 263, Springer-Verlag, pp 311-323, 1987.

[11] P. L. Montgomery “Modular Multiplication without Trial Division”, Mathematics of Computation, vol. 44, no. 170, pp. 519−521, 1985.

[12] 박종연, 최지선, 한동국, 이옥연, “RSA에 대한 향상된 등간격 선택 평문 전력 분석 방법”, 대한전자공학회 2010년 하계종합학술대회, 1877-1880쪽, 한국, 제주도, 2010년 6월.

## 저 자 소 개


**박 종 연**(학생회원)

2010년 국민대학교 수학과 학사 졸업.

2010년~현재 국민대학교 수학과 석사과정

<주관심분야 : 부채널 분석 및 대응법, 화이트 박스 암호, 암호 모듈 고속 구현, 무선 보안>

**한 동 국**(정회원)-교신저자

1999년 고려대학교 수학과 학사 졸업

2002년 고려대학교 수학과 석사 졸업

2005년 고려대학교 정보보호 대학원 박사

2004년 4월~2005년 4월 일본 Kyushu Univ. 방문연구원

2005년 4월~2006년 4월 일본 Future Univ. -Hakodate, Post Doc.

2006년 6월~2009년 2월 한국전자통신연구원 정보보호연구본부 선임연구원

2009년 3월~현재 국민대학교 수학과 조교수

<주관심분야 : 공개키 암호시스템 안전성 분석 및 고속 구현, 부채널 분석, RFID/USN 정보보호 기술>

**이 옥 연**(정회원)

1988년 고려대학교 수학과 학사 졸업

1990년 고려대학교 수학과 석사 졸업

1996년 8월 University of Kentucky 이학박사

1999년 7월~2001년 8월 한국전자통신연구원 선임연구원

2000년 3월~2001년 8월 한국전자통신연구원 팀장

2001년 9월~현재 국민대학교 수학과 교수

<주관심분야 : 스마트 그리드 보안, 무선보안, 4G 보안, 스마트워크 보안>

**최 두 호**(정회원)

1994년 성균관대학교 수학과 학사 졸업

1996년 한국과학기술원 수학과 석사 졸업

2002년 한국과학기술원 수학과 박사

2002년 1월~현재 한국전자통신연구원 선임연구원

<주관심분야 : RFID-USN 정보보호 기술, 페어링 기반 암호 이론, 암호시스템 안전성 증명, 비가환군 암호 이론>