비밀 중간키를 이용한 소프트웨어적 전력분석공격 방어대책

박영구¹ · 김형락² · 이훈재^{3*} · 한덕찬⁴ · 박의영⁴

A Software Power Analysis Countermeasure Using Secrete Intermediate Key

YoungGoo Park¹ · HyeongRag Kim² · HoonJae Lee^{3*} · DeokChan Han⁴ · UiYoung Pak⁴

¹Sacheon Girls High School, Sacheon 664-808, Korea

²Department of Computer Technology and Application, Pohang College, Pohang 791-711, Korea

³Department of Information and Communication Engineering, Dongseo University, Busan 617-716, Korea

⁴Agency for Defense Development, Daejeon, Korea

요 약

전력분석공격은 알려진 값과 마스터키로부터 생성된 숨겨진 값을 입력 받아 연산하는 시점에서 이루어진다. 연산 결과값과 연산 중에 측정된 전력신호의 상관도를 분석하여 숨겨진 값을 찾아내고, 이 찾아낸 값으로 부터 마스터키를 추정할 수 있다. 그러나 전력분석을 가능하게 하는 조건을 바꾸어, 알려진 값과 연산자를 숨기거나, 숨겨진 값으로 부터 마스터키의 추정이 불가능하게 하거나, 연산 결과 값과 전력신호간의 상관도를 매우 낮게 하면 전력분석공격이 매우 어렵게 된다. 이와 같은 전력분석공격을 어렵게 하는 조건을 적용한 비밀 중간키를 이용한 소프트웨어적 방어 대책을 제안한다.

ABSTRACT

Correlation power analysis attack takes place at the point of operating a known value and a hidden value from a master key as an input. The hidden value can be found by analyzing a correlation between the result value and the measured power signal during the operation, which makes it possible to estimate the master key from the hidden value. However, the correlation power analysis attack can be very difficult by changing the conditions that make the power analysis possible, when the known value and the operation is hidden, when it is impossible to estimate the master key from the hidden value, or when the correlation between the result value and the power signal is considerably lowered. Therefore this study proposes a software countermeasure using a secrete intermediate key to which these conditions are applied.

키워드 : 암호시스템, 전력분석공격, AES 공격, 소프트웨어 방어대책, 비밀 중간키

Key word : crypto system, power analysis attack, AES attack, software countermeasure, secrete intermediate key

접수일자 : 2013. 07. 16 심사완료일자 : 2013. 08. 13 게재확정일자 : 2013. 08. 29

* **Corresponding Author** HoonJae Lee (E-mail:hjlee@dongseo.ac.kr, Tel:+82-51-320-1730)

Department of Information and Communication Engineering, Dongseo University, Busan 617-716, Korea

Open Access <http://dx.doi.org/10.6109/jkice.2013.17.12.2883>

print ISSN: 2234-4772 online ISSN: 2288-4165

©This is an Open Access article distributed under the terms of the Creative Commons Attribution Non-Commercial License(<http://creativecommons.org/licenses/by-nc/3.0/>) which permits unrestricted non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited.
Copyright © The Korea Institute of Information and Communication Engineering.

I. 서 론

P. Kocher 등이 제안한 전력 분석[1]은 보안 장치가 암호알고리즘 실행 시 소모하는 전력신호를 이용하여 공격하는 방법으로, 전압 변화의 관찰이 가능한 소규모의 장비로도 공격이 가능하다. 전력신호는 보안장치 내에서 실행되는 암호알고리즘의 연산 값과 높은 상관도를 가진다. 가능한 모든 비밀키를 가정하고, 가정된 비밀 키에 대한 암호알고리즘의 연산 값을 추정하고, 추정된 연산 값의 해밍 값과 측정된 전력신호의 상관도를 계산하면, 올바르게 가정된 키에 대해서는 높은 상관도 값을, 틀리게 가정된 비밀 키에 대해서는 낮은 상관도 값을 나타내게 된다[2-3].

암호알고리즘의 연산이 알려져 있고, 알려진 값과 숨겨진 값을 입력받아 연산을 실행하는 시점에서 전력분석하여 숨겨진 입력값을 찾아내고, 찾아낸 숨겨진 입력값으로부터 마스터키를 알아내는 것이 상관도 전력분석공격이다. 기존의 방어대책은 연산결과값과 전력신호와의 상관도를 낮게하여 공격이 어렵게하는 방법으로 사용하고 있다[4-5]. 그러나 상관도 전력분석공격이 가능한 조건을 바꾸어, 암호알고리즘의 연산을 숨기거나, 연산의 입력값인 숨겨진 비밀 중간키로부터 마스터키의 추정이 불가능하거나, 전력분석 시점에서 연산의 알려진 입력값을 숨기면 상관도 전력분석공격에 대한 방어대책이 될 것이다.

본 논문에서는 대칭 암호시스템에 대한 상관도 전력 분석방법에 대해서 알아보고, AES-128 블록 암호알고리즘[6]이 탑재된 8비트 연산을 하는 스마트카드에 대하여 상관도 전력분석 공격을 한다. 그리고 전력분석 공격을 당하더라도 마스터키의 추정을 어렵게 하는 중간 비밀키를 사용한 대한 소프트웨어적 방어대책을 제안한다. 연산시점에서 상관도 전력분석공격 방어대책에 대하여 살핀 후 마스터키의 추정을 어렵게 하는 비밀 중간키가 적용된 소프트웨어적 방어 대책을 제안하고 결론을 맺는다.

II. 전력분석 공격

2.1. 대칭 암호시스템

대칭 암호시스템은 그림 1과 같은 구조를 가지고 있

으며, 암호알고리즘(encryption algorithm)은 식 (1)과 같이 평문(plain text : p)과 마스터키(master key : k)를 입력 받아 암호문(cipher text : c)을 생성한다.

그림 1. 대칭 암호시스템의 구조

Fig. 1 Structure of symmetric crypto system

$$f(p, k) = c \quad (1)$$

복호알고리즘(decryption algorithm)은 식 (2)와 같이 암호문(c)과 마스터키(k)를 입력으로 하여 평문(p)을 복호하게 된다.

$$f^{-1}(c, k) = p \quad (2)$$

여기서 $f(\cdot)$ 는 암호알고리즘, $f^{-1}(\cdot)$ 은 복호알고리즘이다. 암호시스템에서 암호알고리즘(f), 복호알고리즘(f^{-1})과 암호문(c)은 알려져 있으나, 마스터 키(k)가 알려지지 않은 값이므로, 마스터 키(k)를 모르면 암호문(c)을 복호하여 평문(p)을 알아낼 수 없게 된다. 그러므로 마스터 키(k)를 보호하는 것이 매우 중요하고, 암호시스템에 대한 공격은 이 마스터 키(k)를 알아내는 것이다.

공격자는 암호알고리즘(f)을 알고 있으므로, 암호알고리즘에 평문(p)을 입력하여 암호문(c)을 얼마든지 얻을 수 있게 된다. 그러나 마스터키(k)가 충분히 랜덤한 성질을 가지고, 평문(p)과 암호문(c)사이의 상관도뿐만 아니라 마스터키(k)와 암호문(c)사이의 상관도도 매우 낮도록 암호알고리즘을 설계하면, 알려진 암호문(c), 평문(p)과 암호알고리즘(f)으로 부터 마스터키(k)를 찾아내기가 매우 어렵다.

2.2. 전력분석공격

전력 분석 공격은 그림 2에서 보는 바와 같이, 암호알고리즘이 특정시점(t)에서 식 (3)과 같은 연산을 실행하

는 중에 공격하는 방법이다.

그림 2. 전력분석공격

Fig. 2 Power analysis attack

$$c_t = p_t \odot k_t \quad (3)$$

여기서 $\odot$ 은 연산자, c_t 는 연산값, p_t 는 알려진 값, 비밀 중간키(k_t)는 마스터키(k)로부터 추정이 가능한 값이고, t 는 공격 시점이다. 그리고 k_t 가 알려지면 마스터키(k)값을 찾아 낼 수 있다.

p_t 와 $\odot$ 는 알려져 있으나, c_t 값은 알 수 없으므로, 식 (3)에서 보면 k_t 값을 찾을 수 없다. 그래서 c_t 대신 c_t 와 통계적으로 높은 상관도를 가진 식 (3)을 실행할 때 소모되는 전력신호(T_t)를 측정한다. 마스터키(k)로부터 확산되어 생성된 비밀 중간키의 일부분(k_t)에 대하여 가능한 지 수 만큼 가정하고, 식 (3)을 이용하여 가능한 k_t 각각에 대한 c_t 를 추정한다. c_t 로부터 소모전력을(h_t)를 추정한다. h_t 들과 T_t 와 상관도 분석하여 상관도가 가장 높은 h_t 를 찾으면, 이 h_t 의 추정에 사용된 k_t 가 알고리즘에 사용된 비밀 중간키 값이 된다. 이 비밀 중간키(k_t)를 이용하여 마스터키(k)를 찾게 된다. 예를 들어서 8비트 연산시스템이면 k_t 와 h_t 는 각각 256가지가 될 것이다. 추정된 256가지의 h_t 와 측정된 전력신호 T_t 와 통계적으로 비교하여 상관도가 가장 큰 h_t 을 선택하고, 이 h_t 를 추정한 k_t 를 중간키로 선택하고, k_t 로부터 마스터 키(k)를 계산하게 된다.

상관도 전력신호분석공격은 다음의 4 단계를 거쳐서 공격하게 된다.

1단계 : 전력신호 측정

암호알고리즘을 분석하여 암호알고리즘 실행 중에 알려진 값(p_t)과 비밀 중간키(k_t)가 연산하는 적절한 공격 시점(t)을 선택하고, 전력신호(T_t)를 측정한다.

2단계 : 연산값 추정

공격시점(t)에서 가능한 모든 비밀 중간키(k_{ti})에 대하여 연산값(c_{ti})를 추정한다. 여기서 8비트 연산 시스템인 경우 k_{ti} 는 256가지 ($i=0, \dots, 255$)이다.

3단계 : 소모 전력 추정

연산값(c_{ti})을 이용하여 공격 시점에서의 추정 소모전력(h_{ti})을 계산한다.

4단계 : 통계적 상관도 분석

- 1) h_{ti} 와 T_t 의 통계적 상관도 분석을 한다.
- 2) 올바르게 추정된 h_{ti} 에 대하여는 높은 상관도 값을 가지게 되고, 잘못 추정된 h_{ti} 에 대하여는 낮은 상관도 값을 가지게 되므로, 높은 상관도 값을 갖는 h_{ti} 를 찾는다.
- 3) 2)에서 찾은 h_{ti} 로부터 비밀 중간키(k_{ti})를 얻을 수 있다.
- 4) 비밀 중간키(k_{ti})로부터 마스터 키(k)를 계산한다.

III. AES에 대한 전력분석공격 실험결과

3.1. AES 블록 암호알고리즘

AES는 128비트의 비트열 입력과 128, 192 또는 256비트의 비트열 암호화 키로 구성된 블록 암호알고리즘이며, 각각의 알고리즘을 AES-128, AES-192, AES-256이라 한다.

AES는 기본적으로 8비트 비트열인 바이트 단위로 실행된다. AES는 *AddRoundKey()*, *SubBytes()*, *ShiftRow()*, *MixColumn()* 등의 함수로 구성되어 있으며 블록다이어그램은 그림 3과 같다. 암호화 키 비트열의 크기가 128, 192, 256 이면 반복되는 라운드 수는 각각 10, 12, 14 이다.

그림 3. AES 암호알고리즘
Fig. 3 AES encryption algorithm

3.2. AES 블록 암호알고리즘에 대한 공격

첫 번째 *AddRoundKey()* 함수에서 사용되는 비밀 중간키 키가 마스터키와 동일하여 첫 번째 라운드의 *SubBytes()* 함수의 출력 값 생성 시점을 공격한다 [5]. 가정한 비밀 중간키에 대하여 바이트 단위로 *SubBytes()* 함수의 출력값으로 부터 전력신호를 추정하고, 추정된 전력신호와 측정된 전력신호간의 상관계수를 구하여 비밀 중간키를 찾는다[7-12]. 추정된 전력신호값($x_{k,i}$)과 측정된 전력신호($y_{i,s}$)간의 상관계수($r_{k,s}$)는 식 (4)와 같다.

$$r_{k,s} = \frac{\sum_{i=1}^n (x_{k,i} - \bar{x}_k)(y_{i,s} - \bar{y}_s)}{\sqrt{\sum_{i=1}^n (x_{k,i} - \bar{x}_k)^2 \sum_{i=1}^n (y_{i,s} - \bar{y}_s)^2}} \quad (4)$$

여기서 $r_{k,s}$ 는 k 번째 가정한 비밀 중간키로 추정된 소모전력 값과 측정된 전력신호의 s 번째 샘플들과의 추정 상관계수 값, $x_{k,i}$ 는 k 번째 가정한 비밀 중간키로 i 번째 추정된 전력신호, $\bar{x}_k$ 는 k 번째 가정한 비밀 중간키로 추정된 소모전력값들의 평균값이고, $y_{s,i}$ 는 i 번째 전

력신호의 s 번째 샘플이고, $\bar{y}_s$ 는 측정된 전력신호의 s 번째 샘플들의 평균값이다. 8비트 단위로 공격할 경우 $0 \leq k \leq 255$ 이고, n 은 측정된 전력신호의 갯수, s 는 전력신호의 샘플의 위치이다.

3.3. 실험환경 및 공격 결과

실험 장치를 그림 4와 같이 구성하고, 스마트카드에 *AES-128* 블록 암호알고리즘을 탑재하고, 디지털 오실로스코프를 사용하여 알고리즘 실행 시 소모되는 전력을 측정하고, 컴퓨터의 제어프로그램을 통하여 전력 소모파형을 수집하고 저장한다. 수집된 전력신호의 샘플링 주파수는 50MHz이고 측정 시간은 10msec로, 전력신호 당 획득된 샘플은 500,000개이다

그림 4. 전력신호 수집을 위한 장치
Fig. 4 Power signal acquisition devices

AES-128 블록 암호알고리즘 실행 중 전력신호를 측정하고, 추정된 소모전력 값과 측정된 전력신호사이의 추정 상관계수로 공격하여 사용된 비밀 중간키 중에서 첫 번째 8비트를 찾았다. *AES-128* 블록 암호알고리즘의 첫 번째 *AddRoundKey()* 함수에 사용된 비밀 중간키를 256 가지(0x00 ~ 0xFF)로 가정하고, 가정한 비밀 중간키 각각에 대한 추정된 소모전력 값과 측정된 전력신호 사이의 상관계수들을 계산하고 그림 5에 나타내었다. 그림 5에서 보면 소모전력을 추정한 시점(약 52μs)에서 최대의 상관계수 값을 가짐을 볼 수 있다. 올바르게 가정한 비밀 중간키 값일 때의 상관계수 추정 값을 그림 6에 나타낸다.

그림 5와 그림 6을 비교하면 시간적으로 동일한 위치

에 최대값이 나타남을 관찰할 수 있으며, 이 시각에 AES 블록 암호알고리즘의 *SubBytes()* 함수가 첫 번째 바이트에 대한 연산을 실행하였음을 보여준다. 이러한 과정을 16번 수행하면 AES-128의 비밀 중간키 128 비트(16바이트) 모두를 찾을 수 있다.

그림 5. 전력신호의 상관계수 추정 값 (최대값=0.4196)
Fig. 5 Estimated Correlation coefficient of power signal (Max=0.4196)

그림 6. 올바른 키일 때의 상관계수 (최대값=0.4196)
Fig. 6 Correlation coefficient on correct key (Max=0.4196)

IV. 비밀 중간키를 이용한 소프트웨어적 방어 대책의 제안

암호알고리즘은 비밀 중간키(k_t)로부터 마스터키(k)의 추정이 가능하고, 알고리즘의 실행 연산이 식 (3)에서 보는 바와 같이 p_t , $\odot$ 가 알려져 있으면 상관도 전력 분석으로 비밀 중간키(k_t)를 찾아서 마스터키(k)를 알아내는 것이 가능하다. 그러므로 상관도 전력분석이 가능한 조건을 바꾸어 p_t 와 $\odot$ 를 숨기거나, k 를 k_t 로부터

추정이 불가능하게 하면 상관도 전력분석공격에 대한 방어대책이 될 것이다.

4.1. 연산자($\odot$)를 숨김

연산자($\odot$)를 숨기면 연산값의 추정이 불가능하여 상관도 전력분석 공격이 어려우므로, 상관도 전력분석 공격에 대한 방어대책으로 암호알고리즘이 비공개 되어야 한다.

4.2. 알려진 연산값(p_t)을 숨김

이미 알려진 연산($\odot$)의 실행 중 알려진 연산값(p_t)에 대한 숨김연산을 적용하여 연산값(p_t)을 숨긴다. 그림 7은 p_t 에 숨김연산을 적용한 것이고, 중간값(p')을 생성 후 연산($\odot$)을 실행하게 된다.

그림 7. 알려진 값에 숨김 연산 적용
Fig. 7 Applying hide operation on known value

이 경우 역 숨김연산의 실행이 필요하므로, 역 숨김 연산의 결과 c_t 가 생성되는 시점에서 전력분석 공격이 가능하다.

4.3. 마스터키(k)로부터 비밀 중간키(k_t)의 추정 불가능

그림 8과 같이 마스터키(k)로부터 비밀 중간키(k_t)의 추정 불가능 하고, 비밀 중간키(k_t)로부터 마스터키(k)의 추정 불가능 하도록 알고리즘을 설계하면, 식 (3)으로부터 연산값(c_t)를 얻을 수 없어 상관도 전력 분석공격이 불가능하며, 공격에 의해서 비밀 중간키(k_t)의 일부가 노출되어도 마스터키(k)를 찾기가 어렵게 된다.

그림 8. 비밀 중간키(k_t)의 추정 불가

Fig. 8 Impossible estimation of secret intermediate key

예로 비밀 중간키 생성 시 마스터키(k) 만을 입력 받아 연산하게 되면, 비밀 중간키(k_t)가 알려지더라도 마스터키(k)의 추정이 어렵게 할 수가 있다. 그림 9와 그림 10은 블록암호와 스트림 암호알고리즘에 생성된 비밀 중간키를 적용한 예를 보여준다.

그림 9. 블록암호에 적용된 비밀 중간키

Fig. 9 Secret intermediate key applied block cipher

그림 9의 블록 암호알고리즘에서는 마스터키(k) 만을 이용하여 비밀 중간키(k_t)를 생성한다. 비밀 중간키(k_t)와 알려진 값(p_t)를 입력으로 한 연산 시점에서 전력분석 공격을 하면, 비밀 중간키(k_t)를 찾을 수 있다. 그러나 비밀 중간키(k_t)는 마스터키(k) 만을 이용하여

생성하였으므로, 비밀 중간키(k_t)로부터 마스터키(k)를 찾는 것은 매우 어렵다.

그림 10의 스트림 암호알고리즘에서는 비밀 중간키(k_t)를 초기화 과정에서 마스터키(k) 만을 이용하여 생성하게 된다. 생성된 비밀 중간키(k_t)와 초기벡터(IV)를 이용하여 스트림 암호알고리즘을 초기화하게 된다. 스트림 암호시스템의 전력분석공격은 초기화 과정에서 이루어지게 된다. 초기화 과정에서 전력분석공격을 받게 되더라도 비밀 중간키(k_t)는 마스터키(k) 만으로 생성되었으므로 비밀 중간키로부터 마스터키(k)를 찾는 것은 매우 어렵다.

그림 10. 스트림암호의 초기화 과정에 적용된 비밀 중간키

Fig. 10 Secret intermediate key applied initialization of stream cipher

V. 결 론

상관도 전력분석공격은 암호알고리즘 연산 시 소모 되는 전력이 연산 결과값과 매우 높은 상관도를 갖는 성질을 이용한 방법이다. 암호알고리즘에 대한 상관도 전력분석공격은 비밀 중간키(k_t)로부터 마스터키(k)의 추정이 가능하며, 알고리즘 실행 중에 식 (3)에서 보는 바와 같이 p_t , $\odot$ 가 알려져 있기 때문에 가능하다. AES-128 블록 암호알고리즘이 탑재된 8비트 연산장치인 스마트카드를 상관도 전력분석 공격하여 마스터키(k)의 추정이 가능함을 보여 주었다.

그러나 상관도 전력분석이 가능한 조건을 변경하여, p_i 와 $\odot$ 를 숨기거나, k 를 k_i 로부터 추정이 불가능하게 적용하면 상관도 전력분석 공격에 대한 방어대책이 될 것이다. 연산자($\odot$) 숨김은 암호알고리즘을 공개하지 않아야만 상관도 전력분석 공격에 대해서 안전함을 보여주고, 연산값(p_i)에 대한 숨김 연산의 적용은 역 숨김 연산을 부가적으로 실행하여야 하므로, 부가적 역숨김 연산시 상관도 전력분석공격이 가능하다. 마스터키(k)로부터 비밀 중간키(k_i)의 추정이 어렵고, 비밀 중간키(k_i)로부터 마스터키(k)의 추정이 어려운 중간키 생성 알고리즘을 적용하면 비밀 중간키(k_i)를 찾게 되더라도 마스터키(k)에 대한 추정이 어려워 상관도 전력분석공격에 대한 대책이 될 것이다.

본 논문에서는 알려진 암호알고리즘에 대해서 이루어지는 상관도 전력분석공격에 대한 소프트웨어적인 방어대책으로 비밀 중간키의 적용을 제안 하였다. 제안된 방어대책은 비밀 중간키를 소프트웨어적으로 생성하도록 설계하므로, 부가 장치나 하드웨어의 변경 없이 가능한 장점을 가지고 있다.

상관도 전력분석공격 시점에서 추정 소모전력값(h_i)과 전력신호(T_i)의 상관도가 매우 높기 때문에 상관도 전력분석 공격이 가능하며, h_i 와 T_i 의 상관도를 낮추어 상관도 전력분석 공격이 어렵게 하는 방법에 대하여는 논하지 않았다. h_i 와 T_i 간의 상관도를 낮게 하는 소프트웨어 및 하드웨어적 방법에 대한 더 많은 연구가 필요할 것이다.

감사의 글

본 논문은 2012년도 국방과학연구소 위탁연구 과제 및 2013년도 한국연구재단의 기초연구사업 지원을 받아 수행된 것임(과제번호:2013-071189).

REFERENCES

- [1] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," *Advances in Cryptology, CRYPTO'99, LNCS 1666*, pp. 388-397, 1999.
- [2] J. Jaffe, "Introduction to differential power analysis," *Presented at ECRYPT Summer school on Cryptographic Hardware, Side Channel and Fault Analysis*. 2006.
- [3] M. Rivain, E. Prou. and J. Doget. "Higher-Order Masking and Shuffling for Software Implementation of Block Ciphers," *Cryptographic Hardware and Embedded Systems. CHES 2009, LNCS 5747*, pp. 171-188, 2009
- [4] Ilya Mironov, "(Not So) Random Shuffles Of RCA4", *Advanced in Cryptography, CRYPTO 2002, LNCS 2442*, pp. 304-309, 2002.
- [5] J. Jaffe, "More differential power analysis : Selected DPA attacks," *Presented at ECRYPT Summer school on Cryptographic Hardware, Side Channel and Fault Analysis*, 2006.
- [6] NIST, "Announcing the ADVANCED ENCRYPTION STANDARDS (AES)," *Federal Information Processing Standards Publication 197*, 2001.
- [7] E. Prouff, "DPA attack and s-boxes," *In proceedings of FSE-2005, LNCS 3557*, Springer-Verlag, pp. 424-441, 2005.
- [8] YoungGoo Park, HoonJae Lee, SangJae Moon, "A Constant Pitch Based Time Alignment for Power Analysis with Random Clock Power Trace," *JIPS*, Vol. 18-C, No. 1, pp.7-14, 2011.
- [9] J. Jaffe, "Introduction to Differential Power Analysis", *Presented at ECRYPT Summer school on Cryptographic Hardware, Side Channel and Fault Analysis*. 2006.
- [10] Semenov, O., Vassighi, A., Sachdev, M., Ali K. and Hawkins, C.F. "Burn-in Temperature Projections for Deep Sub-micron Technologies". *In International Test Conference, Proceedings. ITC 2003*. Pp95-104, 2003.
- [11] Po-Chun Liu, Hsie-Chia Chang and Chen-Yi Lee, "Low Overhead DPA Countermeasure Circuit Based on Ring Oscillators". *In IEEE Transactions on Circuits and Systems*. Vol. 57, NO. 7, pp. 546-550, 2010.
- [12] Pramstaller, N., Oswald, E., Mangard, S., Gürkaynak, F. K., and Häne, S., "A masked AES ASIC implementation", *In Proc. Austrochip*, pp. 77-82, 2004.

박영구(YoungGoo Park)

1986년 경북대학교 전자공학과 졸업(학사)
1989년 경북대학교 전자공학과 졸업(석사)
2012년 경북대학교 대학원 전자공학과 (박사)
1989년~1997년 국방과학연구소(선임연구원)
1997년~2008년 창신대학 모바일통신과(조교수)
2010년~2013년 예스테크(연구개발 이사)
2013년~현재 사천여자고등학교 교사
※관심분야 : 정보보호, 정보통신, 부채널공격 등

김형락(HyeongRag Kim)

1992년 경북대학교 전자공학과 졸업(학사)
1994년 경북대학교 전자공학과 졸업(석사)
2010년 경북대학교 전자공학과 졸업(박사)
1994년~1995년 LG전자기술원 연구원
1995년~1996년 (주)문화방송 기술연구소 연구원
1996년~현재 포항대학교 컴퓨터응용계열 부교수
※관심분야 : 정보보안, 암호이론, 채널코딩

이훈재(HoonJae Lee)

1985년 경북대학교 전자공학과 졸업(학사)
1987년 경북대학교 전자공학과 졸업(석사)
1998년 경북대학교 전자공학과 졸업(박사)
1987년~1998년 국방과학연구소 선임연구원/팀장
1998년~2002년 경운대학교 조교수
2002년~현재 동서대학교 컴퓨터정보공학부 교수
※관심분야 : 암호이론, 네트워크보안, 부채널공격, 정보통신/정보네트워크

한덕찬(DukChan Han)

1989년 충남대학교 전자공학과 졸업(학사)
1991년 충남대학교 전자공학과 졸업(석사)
1991년~현재 국방과학연구소 책임연구원
※관심분야 : 데이터통신, 네트워크, 정보보안

박의영(UiYoung Pak)

1982년 연세대학교 전기공학과 졸업(학사)
1988년 연세대학교 전기공학과 졸업(석사)
2003년 연세대학교 전기전자공학과(박사)
1984년~현재 국방과학연구소 책임연구원/팀장
※관심분야 : 데이터통신, 네트워크, 정보보안