논문 2010-47SP-1-17

랜덤 스칼라 대응기법에 대한 부분 공간 기반 전력 분석

(Subspace-based Power Analysis on the Random Scalar Countermeasure)

김 희 석*, 한 동 국**, 홍 석 희***, 이 옥 연****

(HeeSeok Kim, Dong-Guk Han, SeokHie Hong, and Okyeon Yi)

요 약

ECIES와 ECDH의 강력한 DPA 대응방법으로 알려진 랜덤 스칼라 기법은 다양한 전력 분석에 안전한 것으로 알려져 있다. 이 대응방법은 매번 생성되는 난수를 키로 사용해 스칼라 곱셈 연산을 수행하는 하나의 과형에서 이 난수 값을 알 수 있다면 분석이 가능하다. 하지만 이러한 분석 사례가 기존에 없어 아직 안전한 것으로 알려져 있다. 본 논문에서는 이러한 분석을 가능하게 할 수 있는 새로운 전력 분석을 제안한다. 제안하는 분석 기법은 타원곡선의 더블링 연산들을 비교함에 의해 이루어지며 이러한 비교를 용이하게 하기 위해 주성분 분석을 이용한다. 제안하는 주성분 분석을 이용한 부분 공간 기반 전력 분석을 실제로 수행했을 때 기존의 판별 함수의 에러를 완벽하게 제거할 수 있었으며 이를 통해 개인키를 찾아낼 수 있었다.

Abstract

Random scalar countermeasures, which carry out the scalar multiplication by the ephemeral secret key, against the differential power analysis of ECIES and ECDH have been known to be secure against various power analyses. However, if an attacker can find this ephemeral key from the one power signal, these countermeasures can be analyzed. In this paper, we propose a new power attack method which can do this analysis. Proposed attack method can be accomplished while an attacker compares the elliptic curve doubling operations and we use the principle component analysis in order to ease this comparison. When we have actually carried out the proposed power analysis, we can perfectly eliminate the error of existing function for the comparison and find a private key from this elimination of the error.

Keywords : Power Analysis, Side Channel Attack, Random Scalar countermeasure, PCA

I. 서 론

수학적으로 안전한 것으로 알려진 알고리즘조차도 구현 단계에서 고려되지 못한 부가적인 정보의 누출이 있다는 것이 알려졌고, 이로부터 비밀 정보를 알아낼 수 있는 부채널 공격(Side Channel Attack)이 소개되었다[1]. 알려진 부채널 공격에는 결함주입 공격(fault insertion attack)[2~3], 시간 공격(timing attack)[1], 전력 분석 공격(power analysis attack)[4~6], 그리고 전자기 누출 공격(electromagnetic emission attack)[7]등이 있으며 그 중 전력 분석 공격은 가장 강력한 분석법으로 알려져 있다. 전력 분석 공격에는 스마트카드에 물리적 변환을 가하지 않고 단순히 전력신호를 관찰함으로써 사용된 비밀 키의 값을 알아내는 단순 전력 분석 (Simple Power Analysis, SPA)방법과 다수의 전력신호

* 학생회원-주저자, *** 정회원, 고려대학교 정보경영공학전문대학원
(Graduate School of Information Management and Security, Korea University)
** 정회원-교신저자, **** 정회원, 국민대학교 수학과
(Department of Mathematics, Kookmin University)
※ 이 연구에 참여한 연구자(의 일부)는 '2단계 BK21 사업'의 지원비를 받았음.
※ 이 논문은 2008년 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임 (KRF-2008-313-D01028)
접수일자: 2009년6월17일, 수정완료일: 2009년1월4일

를 통계적으로 분석해 비밀 키의 값을 알아내는 차분 전력 분석(Differential Power Analysis, DPA)방법이 있다.

RSA 공개키 암호 시스템의 장기적인 대안으로 최근 활발히 연구되어지고 있는 타원 곡선 암호 시스템(Elliptic Curve Cryptosystem, ECC)을 활용한 암호 스킴 ECIES(Elliptic Curve Integrated Encryption Scheme)[8]와 키 공유 프로토콜 ECDH(Elliptic Curve Diffie-Hellman)[9]도 SPA와 DPA에 취약점을 가진다. 이 두 알고리즘에 대한 SPA는 개인키의 비트 값과 연산방법이 가지는 연관성에 의해 분석이 이루어진다. 즉, 암호 설계자는 이러한 연관성을 제거하기 위해 비트 값에 상관없이 고정된 연산을 수행[10~11]하거나 고정된 연산을 다수 반복하는 구조[12]로 설계해야만 한다. 비록 SPA에 대한 취약성을 고려하여 알고리즘을 설계하더라도 DPA에 대한 안전성을 보장하는 것은 아니다. DPA는 공격자가 암호화 장비가 연산할 중간 값을 예상하고 다수의 파형에 대한 통계치를 이용하는 것으로 장비가 소비하는 전력 파형이 연산되는 데이터 값에 의존한다는 사실에 근거하여 이루어진다. 두 알고리즘의 DPA를 방어하기 위한 대응 방법으로 자주 사용되는 두 가지의 방법이 있다. 첫 번째 방법은 메시지 블라인딩 기법[13~14]으로 타원 곡선의 포인트를 랜덤화 시켜 스칼라 곱셈 연산을 수행하는 기법이며 두 번째 방법은 랜덤 스칼라 기법[15~17]으로 개인키를 랜덤화시켜 스칼라 곱셈 연산을 수행하는 방법이다. 두 방법 모두 중간 연산 데이터를 공격자가 예측하는 것을 불가능하게 한다. 비록 메시지 블라인딩 기법이 DPA에 대한 안전성을 제공할 수 있다 하더라도 이 기법은 고차 차분 전력 분석에 대한 취약성을 지닌 것으로 알려져 있으며 이러한 연구 결과는 2002년 발표되었다[18]. 하지만 랜덤 스칼라 기법은 이러한 고차 차분 전력 분석에 취약점이 드러난 사례가 없으며 지금껏 제시된 취약점도 사용하는 난수의 엔트로피가 충분하다면 여전히 안전한 것으로 여겨질 수 있다. 이러한 랜덤 스칼라 기법에는 scalar randomization(SR)[15], scalar splitting(SS)[16], improved scalar splitting(ISS)[17]의 대표적인 세 가지 방법이 있다. 이러한 랜덤 스칼라 대응 방법들에 적용 가능한 기존의 분석 방법은 템플릿 어택(Template Attack)[19]이 유일하다. 하지만 이러한 공격 방법은 그림 1과 같이 공격 대상 장비 뿐 아니라 공격 대상 장비와 동일한 종류의 트레이닝(Training) 장비에 대해 공

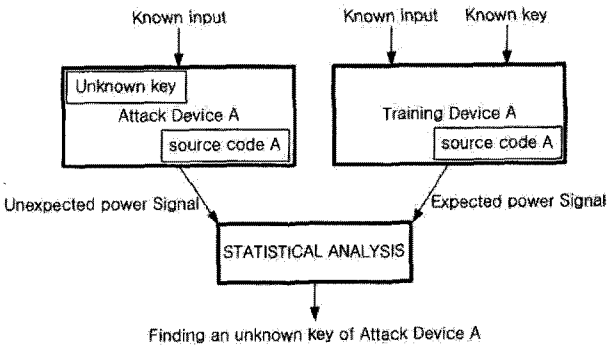


그림 1. 템플릿 어택을 위한 환경 및 시나리오
Fig. 1. Environment and scenario for template attack.

격자가 구현 내용을 모두 알고 있어야 하며 내부의 키도 조절할 수 있다는 가정 하에 이루어지는 분석 방법으로 실질적인 분석 방법으로 판단하기는 어렵다.

앞에서도 언급했듯이 ECIES, ECDH에 DPA 대응 방법으로써 랜덤 스칼라 대응 기법을 적용했다면 이를 분석할 수 있는 실질적인 분석 기법은 아직 존재하지 않는다. 본 논문에서는 이러한 세 가지의 랜덤 스칼라 대응 기법들의 취약점을 현실적으로 드러낼 수 있는 새로운 분석 기법을 제안한다. 제안하는 새로운 분석 기법은 더블링 어택(Doubling Attack)[20]의 가정이 성립할 때 성공되어질 수 있는 분석 방법으로 하나의 스칼라 곱셈 연산 파형에서 나타나는 더블링 연산 신호들을 다른 신호 파형에서 나타나는 더블링 연산 파형들과 비교하며 수행되어진다. 제안하는 분석 기법이 랜덤 스칼라 대응 기법에 대한 분석 방법을 제시하는 것 이외에도 본 논문에서는 더블링 어택의 가정이 실제로 성립하도록 하기 위해 주성분 분석[21]을 이용한 신호처리 기법을 적용한다. 실제 더블링 어택의 가정이 성립하도록 하기 위한 기존의 판별 함수에서 나타났던 많은 에러들이 본 논문에서 제안하는 주성분 분석을 활용한 판별 함수를 사용했을 때 완전히 제거됨을 실험적으로 증명함에 의해 이 가정이 실제 제안하는 분석법에 의해 성립할 수 있음을 증명한다. 이러한 실험적인 증명은 기존에 분석된 사례가 없는 랜덤 스칼라 대응방법을 완벽하게 분석할 수 있음을 의미한다. 본 논문에서 제안하는 분석 기법은 더블링 연산을 비교하는 과정 또는 주성분 분석에서의 선형 필터를 구축하는 과정에서 다수의 파형을 수집해야 하지만 이 다수의 파형을 수집하는 대상 장비는 그림 2와 같이 내부의 개인키를 알 수 없는 공격 대상 장비로 한정되며 따라서 기존의 랜덤 스칼라 대응 방법을 분석할 수 있는 분석 방법인 템플릿 어택과는 차별

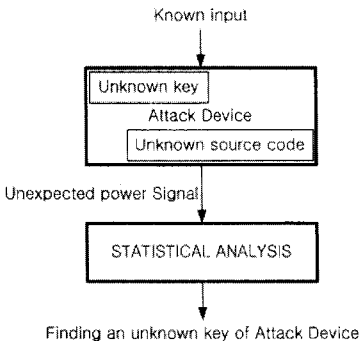


그림 2. 제안하는 분석을 위한 환경 및 시나리오
Fig. 2. Environment and scenario for proposed analysis.

화된다.

본 논문의 구성은 다음과 같다. Ⅱ장은 분석 대상 알고리즘에 대한 설명과 이에 대한 기존의 공격 사례들, 그리고 주성분 분석에 대해 언급한다. Ⅲ장에서는 더블링 어택의 가정이 성립한다고 가정했을 때, 공격 모델을 제시하고 제안하는 분석 시나리오에 의해 랜덤 스칼라 대응방법이 분석될 수 있음을 보인다. Ⅳ장에서는 더블링 어택의 가정을 만족할 수 있는 새로운 판별 함수의 제안과 실험 결과를 통해 제안하는 판별함수가 이 가정을 완벽하게 만족시킴을 증명한다. 마지막으로 본 논문은 Ⅴ장에서 결론짓는다.

1. 스칼라 곱셈 연산에 대한 전력 분석 공격

1985년, Koblitz와 Miller에 의해 제안된 타원곡선 암호 시스템은 DLP(Discrete Logarithm Problem)기반의 암호 시스템으로 스칼라 곱셈 연산(scalar multiplication)을 주요 연산으로 사용한다. 스칼라 곱셈 연산은 타원곡선 위의 점 P에 대해 개인키 d만큼의 덧셈을 수행하는 연산으로서 기본적으로 알고리즘 1과 같이 동작한다.

알고리즘 1. Scalar multiplication
입력 A point P, $d=(d_{m-1}d_{n-2}...d_1d_0)_2$, $d_{m-1}=1$
출력 $Q=dP$
1. $S=P$.
2. For $i=m-2$ down to 0 do :
2.1. $S=2S$.
2.2. If $d_i=1$, $S=S+P$
3. Return S

하지만 이러한 스칼라 곱셈 연산은 특별한 대응법이 없이 구현되어졌을 때, 누출되는 소비 전력에 의해 개인키가 노출될 수 있다. 이러한 부류의 공격을 전력 분석 공격이라 하며, 그 중 가장 강력한 것으로 알려진 분석 방법이 SPA와 DPA이다. SPA란 개인키 d의 비트 값에 의존한 연산의 차이로부터 비밀정보를 알아내는 분석 방법이며 DPA란 공격자가 다수 수집한 전력 파형의 통계치를 이용해 개인키를 찾아내는 분석 방법이다.

알고리즘 1은 개인키의 비트 값이 0일 때 단계 2.1에 해당하는 타원곡선 더블링 연산(Elliptic Curve Doubling, ECDBL)만을 수행하고, 비트 값이 1일 때는 단계 2.1의 ECDBL과 단계 2.2의 에디션 연산(Elliptic Curve Addition, ECADD)을 동시에 수행한다. 이러한 비트 값에 대한 연산식의 차이는 SPA에 취약점을 노출할 수 있다. 즉, 더블링 연산과 에디션 연산에 전력 차이가 시각적으로 구분이 된다면 개인키 d는 쉽게 노출이 가능하다. 하지만 이러한 종류의 분석 방법은 side channel atomicity[12]나 더미 연산[10]등을 사용해 쉽게 방어할 수 있다.

이보다 좀 더 위협적인 공격 방법은 DPA로서 알고리즘 1과 같이 동작하는 스칼라 곱셈 연산에 대한 DPA는 다음의 순서로 이루어진다.

1. L개의 랜덤한 포인트$(P_1, P_2, ..., P_L)$를 입력하여 L개의 스칼라 곱셈 연산 파형$(C_1, C_2, ..., C_L)$을 얻는다.
2. $x=2$, $d'=1$
3. d의 상위 x번째 비트를 0으로 추측하고 $d'=4d'$으로 설정한다.
4. $d'P_1, d'P_2, ..., d'P_L$을 계산하고 각 값의 최하위 비트가 0인 해당 전력 파형들을 X_0로, 1인 해당 전력 파형들을 X_1로 분류한다.
5. X_0, X_1에 포함된 파형들에 대해 각각의 평균 파형 μ_0, μ_1을 구한다.
6. 차분 파형 $D=\mu_1-\mu_0$을 계산하고, 차분 파형에서 피크가 발생하면 0으로 추측한 것이 맞으므로 $d'=d'/2$로, 발생하지 않으면 추측이 틀리므로 $d'=d'/2+1$로 설정한다.
7. $x=m$이면 return d'
8. $x=x+1$로 설정하고 3 단계로 이동.

DPA가 성공할 수 있는 가장 큰 이유는 장비가 연산하는 중간 데이터의 특정 비트 값이 0일 때보다 1일 때 더 큰 전력이 소비되기 때문이다. 따라서 알고리즘 1이

개인키 d의 상위 두 번째 비트가 0일 때 입력 값 P에 대해 $4P$의 연산을 반드시 수행하며 1일 때 $4P$의 연산을 수행하지 않는 특징을 이용, 공격자는 DPA의 단계 4와 같은 분류를 수행해 차분 파형을 구하고 차분이 발생했을 때 두 번째 비트를 0으로써 알 수가 있게 된다. 이러한 과정을 개인키의 비트 수인 m번 반복하면 개인키 d를 찾을 수 있다.

2 타원 곡선의 랜덤 스칼라 대응방법

타원 곡선의 스칼라 곱셈 연산에 대한 DPA는 개인키의 특정비트에 대한 공격자의 추측이 옳다면 공격자가 예상한 중간 값과 실제 전력 소비량간의 연관성이 존재하기 때문에 성공되어질 수 있다. 이러한 연관성을 제거하는 것이 차분 전력 분석 대응법의 고려 시 우선사항이 되고 있으며, 메시지 블라인딩 기법과 랜덤 스칼라 기법이 이러한 역할을 수행하는 대응방법으로 자주 사용되어지고 있다. 메시지 블라인딩 기법은 알고리즘 1의 입력 포인트 P를 매번 다른 값 P'으로 블라인딩 시킨 후 스칼라 곱셈을 수행하고 결과 값 dP'을 언블라인딩 시켜 실제 결과 값 dP을 얻는 기법이다. 하지만 이러한 메시지 블라인딩 기법은 Okeya등이 제안한 이차 차분 전력 분석에 여전히 취약함이 드러났다[18]. 반대로 랜덤 스칼라 대응 기법은 개인키 d를 랜덤한 값으로 매번 변하게 하여 스칼라 곱셈 연산을 수행하는 방법으로 이차 차분 전력 분석에 여전히 안전하다. 이러한 랜덤화 기법으로 자주 사용되는 방법은 다음의 세 가지 기법으로 구분되어진다.

- (SR) $dP=(d+v\#E)P$[15] ($\#E$:커브 위수, v:난수)
- (SS) $dP=vP+(d-v)P$[16] (v:난수)
- (ISS) $dP=[d/v](vP)+(d \bmod v)P$[17] ($[x]$:$x$보다 크지 않은 최대 정수, v:난수)
-

위의 세 가지 방법은 모두 dP의 연산을 수행하지만 각각 매 시행마다 랜덤한 스칼라 곱셈 연산을 수행함에 의해 결과값 dP를 계산한다. 따라서 실제 연산 데이터가 공격자가 예측한 중간 데이터와 다르므로 차분 전력 분석은 실패하게 된다.

Remark 1. (랜덤 스칼라 대응 방법의 위협 요소) 공격자가 한 번의 스칼라 곱셈 연산 xP에 해당하는 파형으로부터 x값을 알아낼 수 있다면 개인키 d는 노출된다. 이 때, x 값은 (SR)의 경우 $d+v\#E$, (SS)의 경우 $v, d-v$, (ISS)의 경우 $v, [d/v], d \bmod v$에 해당한다.

3. 주성분 분석

과도한 차원 문제를 해결하는 좋은 방법은 특징들을 잘 결합해 차원을 줄이는 방법이다. 이러한 특징들을 결합하는 과정에서 선형 결합은 계산이 쉽고 해석학적으로 다루기 쉽기 때문에 자주 사용되어진다. 선형 변환을 통해 고차원 데이터의 주성분을 유지하면서 저차원 데이터로 표현하는 방법이 다양하게 연구되어져 왔으며 주성분 분석(Principal Component Analysis, PCA)은 이러한 선형 변환을 찾는 기법 중 대표적인 방법으로 알려져 있다[21].

주성분 분석이란 최소-제곱 관점에서 데이터를 가장 잘 나타내는 투영을 찾아내는 방법이다. 즉 n차원의 고차원 데이터를 p차원의 저차원 데이터로 선형 변환하여 저차원 데이터의 분산 데이터 값이 최대가 되도록 하는 선형 변환을 찾는다. 이러한 선형 변환을 찾는 문제는 데이터 행렬로부터 얻은 상관행렬(correlation matrix)의 고유벡터(eigenvectors)를 찾아냄에 의해 이루어진다. s개의 n차원 샘플 $(S_1, S_2, ..., S_s)$을 갖는 표본에 대해 주성분 분석을 이용해 선형 변환을 찾는 과정은 다음과 같다.

- 각 샘플 $S_i(t)(1 \le i \le s, 1 \le t \le n)$에 대해 u개의 전력 파형을 얻고 이 전력 파형의 평균 파형 $X_i(t)$를 얻는다.
- $E(X(t)) = \sum_{i=1}^{s} S_i(t)\ (1 \le t \le n)$를 계산한다.
- 데이터 행렬 $U_{n \times s}$를 $[X_1 - E(X); \ldots; X_s - E(X)]$로 설정한다.
- 상관 행렬 UU^T를 구하고 $UU^T = VCV^{-1} = VCV^T$를 만족하는 고유벡터 행렬 V와 고유값 행렬 C를 구한다.
- p개의 큰 고유값에 해당하는 고유벡터들로 선형 변환 행렬 $G_{n \times p}$를 구성한다.

하지만 이러한 과정은 n값이 큰 고차원의 문제일 때 $n \times n$ 크기의 상관 행렬 UU^T의 고유벡터 행렬과 고유값 행렬을 구하는 연산을 필요로 하며 일반적으로 크기가 큰 전력파형 같은 경우 실제로 이 연산은 불가능하다. 따라서 이러한 고차원 문제의 경우 비교적 작은 $p \times p$ 크기의 $\frac{1}{s}U^TU$ 행렬에 대한 고유벡터 행렬과 고

유값 행렬을 구함에 의해 해결해야 하며 알고리즘 2와 같이 변형된다[22].

알고리즘 2. Principal Component Analysis

1. 각 샘플 $S_i(t)(1 \le i \le s, 1 \le t \le n)$에 대해 u개의 전력 파형을 얻고 이 전력 파형의 평균 파형 $X_i(t)$를 얻는다.
2. $E(X(t)) = \sum_{i=1}^{s} S_i(t)\ (1 \le t \le n)$를 계산한다.
3. 데이터 행렬 $U_{n \times s}$를 $[X_1 - E(X); \ldots; X_s - E(X)]$로 설정한다.
4. $\frac{1}{s} U^T U$를 구하고 $\frac{1}{s} U^T U = VCV^{-1} = VCV^T$를 만족하는 고유벡터 행렬 V와 고유값 행렬 C를 구한다.
5. p개의 큰 고유값에 해당하는 고유벡터들로 선형 변환 행렬 $G_{n \times p}$를 구성한다.

Ⅲ. 랜덤 스칼라 대응 방법 분석 시나리오

1. 공격 모델

그림 3은 세 가지의 랜덤 스칼라 대응방법(SR, SS, ISS)의 구성도를 도식화한 것이다. 세 가지의 랜덤 스칼라 대응방법 모두 입력 포인트 Q에 대해서 출력 포인트 dQ를 연산하며 공통적으로 System A 연산 블록을 사용한다.

그림 3에서의 System A 연산 블록의 구성도는 그림 4와 같으며 내부적으로 생성한 난수 v로부터 세 개의 단명의 키 k_1, k_2, k_3를 생성해 낸다. 이 단명의 키를 생성하는 방법은 함수 f에 의해 결정되며 각 대응방법에

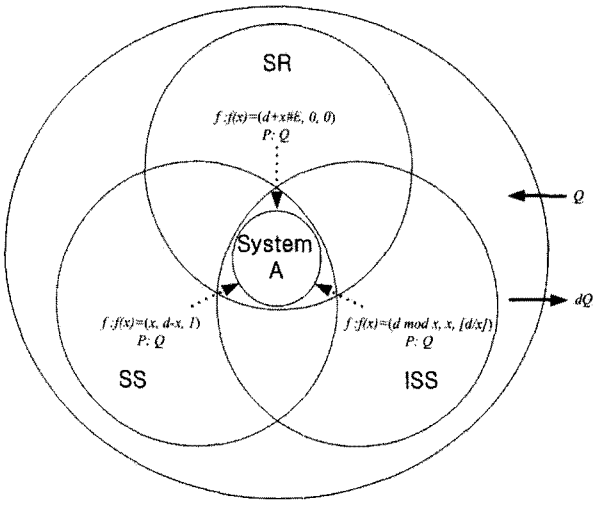


그림 3. 랜덤 스칼라 대응방법들의 전체 구성도
Fig. 3. The entire structure of random scalar countermeasures.

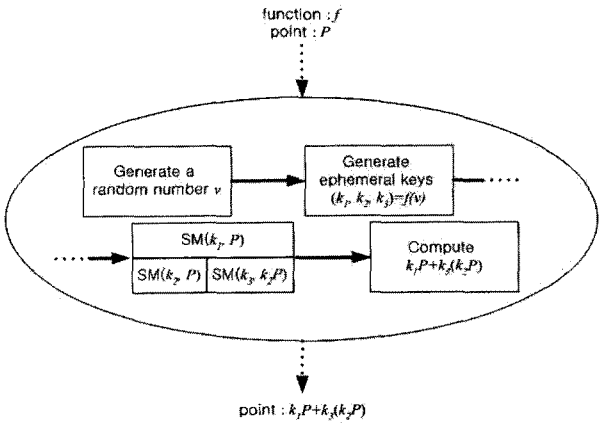


그림 4. System A
Fig. 4. System A.

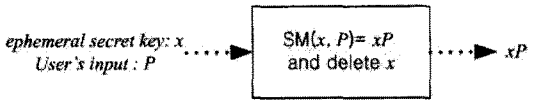


그림 5. 공격 모델(SM 모듈)
Fig. 5. Attack model(SM module).

따라 다음과 같이 결정된다.

- (SR) $f(v) = (k_1, k_2, k_3) = (d + v\#E, 0, 0)$
- (SS) $f(v) = (k_1, k_2, k_3) = (v, d - v, 1)$
- (ISS) $f(v) = (k_1, k_2, k_3) = (d \bmod v, v, [d/v])$

System A가 동작하기 위해서는 단명의 키 x와 입력 포인트 P에 대해서 스칼라 곱셈 연산을 수행하는 SM 모듈이 있어야 한다. 이 SM 모듈을 도식화하면 그림 5와 같으며, 이 SM 모듈에서 x가 노출된다면 전체 시스템이 공격된다.

단명의 키 x와 입력 포인트 P에 대하여 xP를 연산하는 스칼라 곱셈 연산 모듈 SM에서 얻은 전력 파형으로부터 공격자가 단명의 비밀키 x를 알 수 있는 방법이 존재한다면 이는 공격자가 System A에서 k_1, k_2, k_3를 알 수 있음을 의미하며 이는 전체 구성도에서 다음과 같이 개인키 d를 알 수 있음을 의미한다.

- (SR) $d = k_1 \bmod \#E$
- (SS) $d = k_1 + k_2$
- (ISS) $d = k_1 + k_2 k_3$
-

따라서 본 절에서는 SM 모듈을 분석할 수 있는 시나리오를 제시함에 의해 랜덤 스칼라 대응방법이 분석됨을 보인다.

2. 공격의 가정과 기존 판별함수

제안하는 부분공간 기반 전력 분석 공격은 다음의 더블링 어택의 가정이 성립될 때 이루어질 수 있다.

Assumption 1. (Doubling Attack의 가정) 암호화 장비가 연산한 두 개의 타원곡선 더블링 연산에 해당하는 파형으로부터 공격자는 같은 더블링 연산에 대한 파형인지 다른 더블링 연산에 대한 파형인지 구별할 수 있다.

*Assumption 1*에서 두 더블링 연산 파형 $D_1(t), D_2(t)$에 대해 같은 더블링 연산 파형과 다른 더블링 연산을 구별하기 위한 기존의 판별 함수는 다음과 같다(n:신호 D_1, D_2의 길이)[20].

$$Disc.(D_1, D_2) = \frac{1}{n}\sum_{j=1}^{n}(D_1(j) - D_2(j))^2 \quad (1)$$

즉, 두 더블링 연산에 해당하는 전력 파형에서 식 (1)의 판별 값이 특정 값보다 작으면 두 더블링 연산을 같은 연산으로 판단하고, 특정 값보다 크면 다른 연산으로 공격자는 판단한다. 하지만 실제 노이즈가 많은 장비에서는 이 판별 함수를 이용해 구분이 불가능하거나 많은 에러를 가지게 되며, 이를 해결하기 위해서는 저역 통과 필터링(Low Pass Filtering)과 같은 방법을 사용해야만 한다[23]. 하지만 *Remark 1*에서 기술했듯이 단명의 키를 사용하는 랜덤 스칼라 대응방법에서 이러한 노이즈 제거 방법을 사용하는 것은 불가능하다.

본 절에서는 우선 두 더블링 신호 D_1, D_2에 대해 *Assumption 1*이 성립하도록 하는 판별함수 $Disc_New(D_1, D_2)$가 존재한다고 가정하고 이를 이용해 랜덤 스칼라 대응 방법을 분석할 수 있는 분석 시나리오를 제안하고 다음 절에서 이 가정을 만족할 수 있는 $Disc\_New$ 함수를 제안한다.

3. 분석 시나리오

본 논문에서 제안하는 공격 방법은 하나의 스칼라 곱셈 연산 파형에 포함된 타원곡선 더블링 연산 신호와 다른 스칼라 곱셈 연산 파형에 포함된 타원곡선 더블링 연산 신호를 비교하며 수행되어진다. 제안하는 공격 방법은 단순 전력 분석 대응법의 종류에 상관없이 적용 가능하다. 하지만, 그 종류에 따라 수행 방법은 약간의 차이를 가진다. 본 논문에서는 쉬운 기술을 위해 단순 전력 분석 대응법으로서 side channel atomicity를 적용한 경우를 고려한다[12]. 물론 더미연산[10]이나 몽고메리 레더(Montgomery Ladder)[11]와 같은 SPA 대응 기법에 대해서도 이러한 분석은 쉽게 응용 가능하다. side channel atomicity란 기본 연산 블록(atomic block)을 지정하고 연산식이 다른 두 연산을 기본 연산의 반복적인 구조로 설계하는 방식이다. 타원 곡선의 경우 더블링 연산과 에디션 연산의 기본 연산 블록(예: 곱셈 연산 1회, 덧셈 연산 2회, 보수 연산 1회)을 구성하고 n_D개의 기본 연산 블록으로 더블링 연산을, n_A개의 기본 연산 블록으로 에디션 연산을 구성한다. 이는 알고리즘 1의 비트 값에 따라 나타나는 연산차이(0 : ECDBL, 1 : ECDBL, ECADD)를 기본 연산 블록의 반복적인 수행에 의해 공격자가 구분 불가능하도록 하여 단순 전력 분석에 안전하게 하기 위함이다. 일반적으로 하나의 전력 파형에서 atomic block은 시각적으로 충분히 구분 가능하며 실제 실험에서도 쉽게 구분될 수 있었다.

Atomic block을 구분한 후 랜덤 스칼라 대응 방법에 대한 공격은 다음 순서로 진행된다. 아래의 공격 방법은 단명의 키 x에 대해 알고리즘 1에 따라 공격 모델인 SM에서 xP를 연산하는 하나의 전력 파형 C_x로부터 x 값을 알아내는 방법으로 그림 5의 공격모델을 분석할 수 있음을 보인다.

- 공격자가 x의 상위 $m-w-1$비트 $x_{m-1}x_{m-2}\cdots x_{w+1}$를 안다고 가정하자.
- 공격자는 x_w을 얻기 위해 그림 3의 전체 구성도에서 입력 포인트 Q를 $(\sum_{i=w+1}^{m-1} x_i 2^{i-w})P$로 선택해 SM 모듈이 소비한 전력 파형 C_{w0}를 얻고, 두 번째로 Q를 $(\sum_{i=w+1}^{m-1} x_i 2^{i-w}+1)P$로 선택해 파형 C_{w1}을 얻는다.
- C_x의 $m-w$번째 더블링 연산 파형으로 예상되어지는 $D_{x,m-w}$(ECDBL($(\sum_{i=w+1}^{m-1} x_i 2^{i-w})P$))와 C_{w0}의 첫 번째 더블링 연산 파형 D_{w0}(ECDBL($(\sum_{i=w+1}^{m-1} x_i 2^{i-w})P$))으로부터 식 (2)를 계산한다.

$$ND_0 = Disc\_New(D_{k,m-w}, D_{w0}) \quad (2)$$

$D_{x,m-w}$는 C_x에서 $(m-w-1)\times n_D + \sum_{i=w+1}^{m-1} k_i \times n_A + 1$번째 atomic block부터 $(m-w)\times n_D + \sum_{i=w+1}^{m-1} k_i \times n_A$번째 block까지 n_D개의 block으로 구성된다. 반면, D_{w0}는

C_{w0}에서 처음부터 n_D개의 atomic block으로 구성된다.

- C_x의 $m-w$번째 더블링 연산 파형으로 예상되어지는 $D_{x,m-w}$(ECDBL($(\sum_{i=w+1}^{m-1} x_i 2^{i-w}+1)P$))와 C_{w1}의 첫 번째 더블링 연산 파형 D_{w1}(ECDBL($(\sum_{i=w+1}^{m-1} x_i 2^{i-w}+1)P$))으로부터 식 (3)를 계산한다.

$$ND_1 = Disc\_New(D_{k,m-w}, D_{w1}) \tag{3}$$

$D_{x,m-w}$는 C_x의 $(m-w-1)\times n_D+(\sum_{i=w+1}^{m-1} k_i+1)\times n_A$ +1번째 atomic block부터 $(m-w)\times n_D+(\sum_{i=w+1}^{m-1} k_i+1)\times n_A$번째 block까지 n_D개의 block으로 구성된다. 반면, D_{w1}는 C_{w1}에서 처음부터 n_D개의 atomic block으로 구성된다.

- $ND_0 < ND_1$이라면 x의 상위 $(m-w)$번 째 비트 x_w를 0으로 정하고 그렇지 않으면 1로 선택한다.
- 위의 단계를 반복해 x의 최상위 두 번째 비트부터 모든 비트를 알아낸다.

위의 과정에서 x_w가 0이라면 식 (2)에서 C_x의 $m-w$번째 더블링 연산 파형인 $D_{x,m-w}$는 알고리즘 1에 따라 $(\sum_{i=w+1}^{m-1} x_i 2^{i-w})P$에 대한 더블링 연산 파형으로 구성되어진다. D_{w0}도 같은 연산에 대한 파형으로써 *Assumption 1*이 성립한다면 $D_{x,m-w}$와 D_{w0}의 판별 값인 ND_0 값은 상당히 작은 값이 될 것이다. 하지만 이 경우 식 (3)에서는 다른 연산에 대한 두 더블링 파형의 판별 값을 연산하는 것이므로 ND_1은 상당히 큰 값이 된다. 반대로 x_w가 1이라면 식 (3)에서 C_x의 $m-w$번째 더블링 연산 파형인 $D_{x,m-w}$는 알고리즘 1에 따라 $(\sum_{i=w+1}^{m-1} x_i 2^{i-w}+1)P$에 대한 더블링 연산 파형으로 구성되어진다. D_{w1}도 같은 연산에 대한 파형으로써 $D_{x,m-w}$와 D_{w1}의 판별 값인 ND_1 값은 상당히 작은 값이 될 것이다. 따라서 ND_0 값과 ND_1 값을 비교함에 의해 공격자는 비트 값 x_w을 알 수 있다. 이러한 공격 방법을 x의 최상위 두 번째 비트 값부터 순차적으로 적용함에 의해 공격자는 x의 모든 비트 값을 알 수 있다.

Ⅳ. 부분 공간 기반 판별 함수

1. 새로운 판별 함수의 구성

본 절에서는 *Assumption 1*에서의 분류 성공 확률을 높이기 위해 주성분 분석을 통해 생성한 선형 변환 행렬(선형 필터) G로부터 새로운 판별함수 *Disc_New*를 구성한다. 우선 선형 필터 G는 다음 순서로 생성된다.

그림 3의 전체 시스템에서 랜덤한 메시지 P_1을 반복적으로 u회 입력 값으로 넣는다. 이로부터 공격 모델인 SM 모듈이 소비한 스칼라 곱셈 파형들로부터 가장 먼저 나타나는 타원 곡선 더블링 연산(ECDBL(P_1))에 해당하는 파형 u개를 수집해 평균 파형 X_1을 구한다.

다른 랜덤한 메시지 P_2, ..., P_s에 대해서도 위의 과정을 반복하여 각각의 평균 파형 X_2, ..., X_s를 얻는다(본 논문에서는 $s=64$의 임의의 표본을 사용하였다.).

알고리즘 2의 단계 2, 3, 4, 5를 수행해 행렬 G를 생성한다.

위의 과정을 통해 생성된 선형 필터 G가 만족해야하는 기능을 도식화하면 그림 6과 같다.

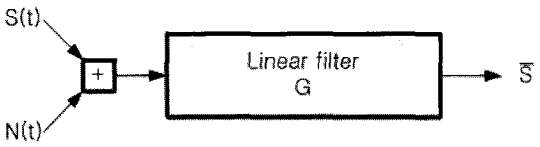


그림 6. 선형 필터 G를 활용한 잡음 제거
Fig. 6. Noise reduction using a linear filter G.

그림 6에서의 선형 필터 G를 활용해 신호 압축 기능 외에 잡음 제거를 수행함으로써 *Disc_New* 함수가 만족하고자 하는 기능은 식 (4)과 같다.

$$Disc\_New(S_1+N_1, S_1+N_2) \ll Disc\_New(S_3+N_3, S_4+N_4) \tag{4}$$

즉, 같은 연산에 대한 두 신호의 *Disc_New* 값이 다른 연산에 대한 두 신호의 *Disc_New* 값에 비해 상당히 작도록 하는 기능을 제안하는 판별 함수는 수행해야만 한다.

본 논문에서는 이러한 기능을 수행하는 새로운 판별 함수를 식 (5)와 같이 정의한다.

$$Disc\_New(D_1, D_2) = Disc.(G^T D_1, G^T D_2) \tag{5}$$

식 (5)의 새로운 판별함수는 선형 변환 행렬 G에 대

해 n개의 사전 계산 값을 이용하여 *Theorem 1*과 같이 계산되어질수 있다.

Theorem 1. 주성분 분석에 의해 생성된 선형 변환 행렬 $G^T=(g_{ij})_{p\times n}$*에 대해* $\|(G^T)i\|$*를* $\sum_{i=1}^{p} g_{ij}^2$*로서 정의하면,* $Disc\_New(D_1, D_2)=\frac{1}{p}\sum_{j=1}^{n}\|(G^T)i\|(D_1(j)-D_2(j))^2$ *이다.*

proof)

$$
\begin{aligned}
Disc\_New(D_1, D_2) &= Disc.(G^T D_1, G^T D_2) \\
&= \frac{1}{p}\sum_{i=1}^{p}\sum_{j=1}^{n}(g_{ij}D_1(j)-g_{ij}D_2(j))^2 \\
&= \frac{1}{p}\sum_{i=1}^{p}\sum_{j=1}^{n} g_{ij}^2(D_1(j)-D_2(j))^2 \\
&= \frac{1}{p}\sum_{j=1}^{n}(D_1(j)-D_2(j))^2\sum_{i=1}^{p} g_{ij}^2 \\
&= \frac{1}{p}\sum_{j=1}^{n}\|(G^T)i\|(D_1(j)-D_2(j))^2
\end{aligned}
$$

■

2. 제안하는 판별함수를 이용한 더블링 어택의 가정의 성립

*Assumption 1*이 성립한다면 앞 절에서 제안한 공격 방법에 따라 랜덤 스칼라 대응방법의 비밀 정보는 노출이 될 수 있다. 즉, 두 알고리즘을 분석하기 위해 남은 것은 *Assumption 1*이 현실적으로 성립할 수 있음을 보이는 것이다. 앞에서도 설명했듯이 *Assumption 1*을 성립하도록 다수의 파형을 이용하는 것은 알고리즘의 특성상 불가능하며 따라서 본 논문에서는 주성분 분석을 활용해 하나의 파형, 즉, 비교하고자 하는 단지 두 개의 파형으로부터 *Assumption 1*이 성립함을 실험적으로 증명한다. 이러한 증명을 위해 기존 *Disc.*함수의 에러를 제안하는 *Disc_New*함수가 완전히 제거할 수 있음을 본 절에서 증명한다.

본 실험은 스칼라 곱셈 연산이 구현되어있는 스마트 카드를 대상으로 수행되어졌다. 본 실험을 수행하기 위해 임의의 같은 더블링 연산 100,000개와 다른 더블링 연산 100,000개에 대한 파형 쌍을 얻어 판별 값을 구별해 보았다. 이 100,000개의 쌍에 대해 기존의 판별 함수 *Disc.* 값을 연산한 실험 결과는 다음 그림 7과 같다.

그림 7은 같은 연산에 대한 100,000개의 *Disc.* 값의 분포(X_1, 왼쪽 분포)와 다른 연산에 대한 100,000개의 *Disc.*값의 분포(X_2, 오른쪽 분포)를 나타낸 것이다. 본

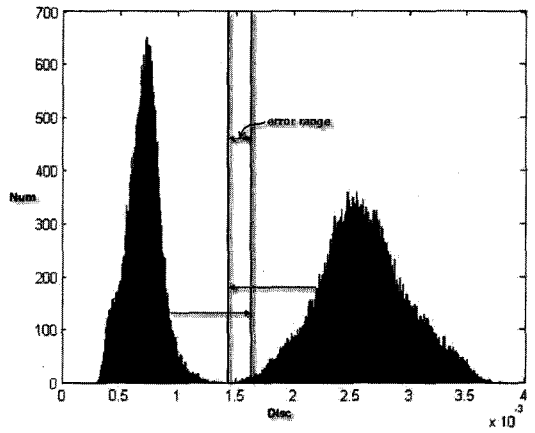


그림 7. *Disc.* 값의 분포도

Fig. 7. The distribution of *Disc.* values.

논문에서는 $X_2 < \max(X_1)$과 $X_1 > \min(X_2)$일 때 에러가 발생한다고 정의한다. 실제 100,000개의 X_2의 원소 중 $\max(X_1)$보다 작은 값을 가지는 원소의 개수는 543개가 존재했으며 X_1의 원소 중 $\min(X_2)$보다 큰 값을 가지는 원소의 개수는 17개가 존재했다. 실제로 기존의 *Disc.* 값을 이용해 판별이 잘 안되는 경우는 이와 같이 미비하지만 전체 160비트의 개인키를 사용하는 스칼라 곱셈 연산의 경우 160번의 비교가 모두 성공해야만 하고 중간에 에러가 발생한다면 분석을 새로 수행해야만 하기 때문에 이 미비한 에러 확률을 무시할 수 없다.

본 논문에서 제안하는 주성분을 활용한 부분 공간 기반 전력 분석 방법은 이러한 에러 확률을 완벽하게 제거할 수 있었다.

본 논문에서 제안하는 분석 방법을 수행하기 위해 G

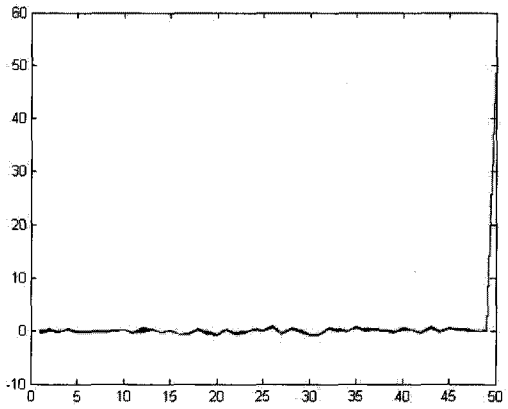


그림 8. 같은 연산에 대한 60개의 다른 전력 파형의 선형 변환 후 벡터 값

Fig. 8. Vectors after transforming 60 power traces according to same operation using linear filter.

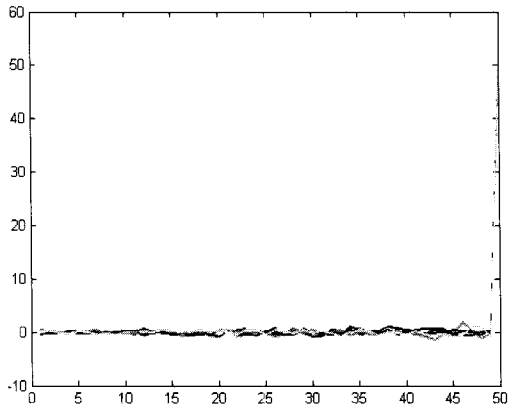


그림 9. 다른 연산 다섯 개에 대한 선형 변환 후 벡터 값

Fig. 9. Vectors after transforming 5 power traces according to different operations using linear filter.

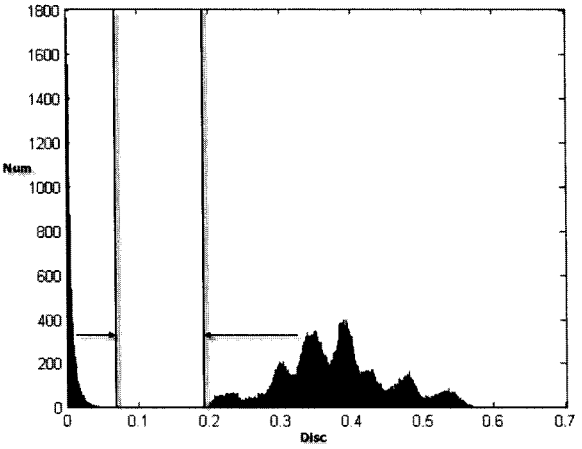


그림 10. *Disc_New* 값의 분포도

Fig. 10. The distribution of *Disc_New* values.

행렬을 생성하는 과정에서 50 차원의 주성분을 선택하고 본래의 전력 파형을 선형 변환했다. 다음 그림은 동일한 입력 값에 대해 더블링 연산을 60번 수행한 후, 60개의 전력파형을 겹쳐서 그린 그림이다.

선형 변환 전 랜덤해 보이던 같은 연산에 대한 전력 파형들은 그림 8에서 보는 바와 같이 거의 동일한 벡터 값으로 변환됨을 확인할 수 있다. 실제 다른 연산 다섯 개에 대해 각각 60번의 연산을 수행한 후, 수집한 전력 파형들의 선형 변환을 수행했을 때는 그림 9와 같이 시각적으로 구분이 가능하였다.

Disc. 값의 분포를 확인 했을 때와 마찬가지로 *Disc_New* 값의 분포를 확인하기 위해 같은 더블링 연산 100,000개와 다른 더블링 연산 100,000개에 대한 파형 쌍을 얻어 판별 값을 구별해 보았다. 결과는 그림 10과 같았다.

제안하는 분석법을 이용했을 때, 같은 연산에 대한 100,000개의 *Disc_New* 값의 분포(X_1, 그림 10의 왼쪽 분포)에서 $\max(X_1)$ 값은 0.0791 값이었으며 다른 연산에 대한 100,000개의 *Disc_New* 값의 분포(X_2, 그림 10의 오른쪽 분포)에서 $\min(X_2)$의 값은 0.1893 값을 가졌다. 즉, 에러를 가지는 값은 존재하지 않았으며 두 분포가 확연하게 구분되었다. 이는 *Assumption 1*이 제안하는 판별 방법에 의해 성립함을 증명한다.

VI. 결 론

본 논문은 타원곡선 암호시스템을 이용한 암호화 스킴 ECIES와 키 공유 프로토콜 ECDH가 DPA 대응 기법으로서 랜덤 스칼라 대응 기법들(SR, SS, ISS)을 사용했을 때 이를 분석할 수 있는 공격 방법을 제안한다. 또한 에러를 줄이기 위해 주성분 분석을 활용함으로써 기존의 판별함수의 에러를 완벽하게 제거할 수 있음을 보이며 이로부터 랜덤 스칼라 대응기법을 적용한 경우에도 개인키를 찾아낼 수 있음을 증명한다.

참 고 문 헌

[1] P. Kocher, J. Jaffe, and B. Jun, "Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Others Systems, " CRYPTO 1996, LNCS 1109, pp. 104-113, Springer-Verlag, 1996.

[2] Bellcore Press Release, "New threat model breaks crypto codes," or D. Boneh, R. A. DeMillo, and R. J. Lipton, "On the importance of checking cryptographic protocols for faults", EUROCRYPT 1997, LNCS 1233, pp. 37-51, Springer-Verlag, 1997.

[3] S. M. Yen, S. J. Kim, S. G. Lim, and S. J. Moon, "A countermeasure against one physical cryptanalysis May Benefit Another Attack," ICISC 2001, LNCS 2288 , pp. 414-427, Springer-Verlag, 2001.

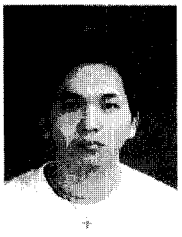
[4] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," CRYPTO 1999, LNCS 1666, pp. 388-397, Springer-Verlag, 1999.

[5] P. Kocher, J. Jaffe, and B. Jun, "Introduction to differential power analysis and related attacks," Available online at http://www.cryptography.com /dpa/technical, 1998.

[6] T. S. Messerges, E. A. Dabbish, and R. H.

Sloan, "Power analysis attacks on modular exponentiation in Smart cards," CHES 1999, LNCS 1717, pp. 144-157, Springer-Verlag, 1999.
[7] D. Agrawal, B. Archambeault, J. R. Rao, and P. Rohatgi, "The EM Side-Channel(s)," CHES 2002, LNCS 2523, pp. 29-45, Springer-Verlag, 2003
[8] Certicom Research, Standards for efficient cryptography, SEC 1: Elliptic Curve Cryptography, Version 1.0, September 20, 2000.
[9] NIST, Special Publication 800-56A, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, March, 2006.
[10] J. S. Coron, "Resistance against differential power analysis for Elliptic Curve Cryptosystems," CHES 1999, LNCS 1717, pp.292-302 , Springer-Verlag, 1999.
[11] T. Izu and T. Takagi, "A Fast Parallel Elliptic Curve Multiplication Resistant against Side Channel Attacks," PKC 2002, LNCS 2274, pp. 280-296, Springer-Verlag, 2002.
[12] B. Chevallier-Mames, M. Ciet, and M. Joye, "Low-cost solutions for preventing simple side-channel analysis: side-channel atomicity," IEEE Trans. Computers, Vol. 53, No. 6, pp. 760-768, 2004.
[13] H. Mamiya, A. Miyaji, and H. Morimoto, "Efficient Countermeasures Against RPA, DPA, and SPA," CHES 2004, LNCS 3156, pp. 343-356, Springer-Verlag, 2004.
[14] K. Itoh, T. Izu, and M. Takenaka, "Improving the Randomized Initial Point Countermeasure Against DPA," ACNS 2006, LNCS 3989, pp.459 - 469, Springer-Verlag, 2006.
[15] J.S. Coron, "Resistance against Differential Power Analysis for Elliptic Curve Cryptosystems," CHES 1999, LNCS 1717, pp. 292-302, Springer-Verlag, 1999.
[16] C. Clavier and M. Joye, "Universal exponentiation algorithm - A first step towards provable SPA-resistance -," CHES 2001, LNCS 2162, pp. 300-308, Springer-Verlag, 2001.
[17] M. Ciet and M. Joye, "(Virtually) Free randomization technique for elliptic curve cryptography", ICICS 2003, LNCS, 2836, pp. 348-359, Springer-Verlag, 2003.
[18] K. Okeya and K. Sakurai, "A Second-Order DPA Attack Breaks a Window method based Countermeasure against Side Channel Attacks," ISC 2002, LNCS 2433, pp. 389-401, Springer-Verlag, 2002.
[19] M. Medwed, E. Oswald, "Template Attack on ECDSA," WISA 2008, LNCS 5379, pp. 14-27, Springer-Verlag, 2008.
[20] P. A. Fouque and F. Valette, "The Doubling Attack - Why Upwards Is Better than Downwards", CHES 2003, LNCS 2779, pp. 269 - 280, Springer-Verlag, 2003.
[21] I. T. Jolliffe. Principal Component Analysis. Springer-Verlag, New York, 1986.
[22] K. Fukunaga. Introduction to Statistical Pattern Recognition. Elsevier, New York, 1990.
[23] N. Homma, A. Miyamoto, T. Aoki, A. Satoh, and A. Shamir, "Collision-Based Power Analysis of Modular Exponentiation Using Chosen-Message Pairs," CHES 2008, LNCS 5154, pp.15-29 , Springer-Verlag, 2008.

저 자 소 개



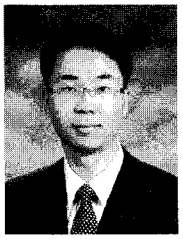
김 희 석(학생회원)

2006년 2월 연세대학교 수학과 학사

2008년 2월 고려대학교 정보보호대학원 공학석사

2008년~현재 고려대학교 정보보호대학원 박사과정

<주관심분야 : 부채널 공격, 암호시스템 안전성 분석 및 고속구현, 암호칩 설계 기술>



한 동 국(정회원)

1999년 2월 고려대학교 수학과 학사

2002년 2월 고려대학교 수학과 이학석사

2005년 2월 고려대학교 정보보호대학원 공학박사

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

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

2006년 6월~2009년 2월: 한국전자통신연구원 정보보호연구단 선임연구원

2009년 3월~현재: 국민대학교 수학과 조교수

<주관심분야: 암호시스템 안전성 분석 및 고속구현, 부채널 분석, RFID/USN 정보보호 기술>

홍 석 희(정회원)

1995년 2월 고려대학교 수학과 학사

1997년 2월 고려대학교 수학과 이학석사

2001년 2월 고려대학교 수학과 이학박사

1999년 8월~2004년 2월 (주)시큐리티 테크놀로지스 선임연구원

2003년 3월~2004년 2월 고려대학교 시간강사

2004년 4월~2005년 2월 K.U. Leuven 박사후 연구원

2005년 3월~2008년 8월 고려대학교 정보경영공학전문대학원 조교수

2008년 9월~현재 고려대학교 정보경영공학전문대학원 부교수

<주관심분야: 대칭키 암호 알고리즘, 공개키 암호 알고리즘, 포렌식>

이 옥 연(정회원)

1988년 2월 고려대학교 수학과 학사

1990년 2월 고려대학교 수학과 이학석사

1996년 8월 Univ. of Kentucky Ph.D.

1999년~2001년 ETRI 선임연구원

2001년~현재 국민대학교 수학과 부교수

<주관심분야 : 이동통신 정보보호, 컴퓨터 보안>