정 보 보 호 학 회 지
제 30 권 제1호, 2020. 2

# ISO 비침투공격 시험방법론 표준화 동향

박 태 환*, 박 진 형*, 장 상 운**

요 약

비침투보안은 암호모듈 검증제도와 CC 평가 등에서 암호 시스템이 만족해야 하는 보안 요구사항 중 하나이다. 최근 미국 CMVP 제도는 기존 FIPS 140-2 기반의 시험기준을 ISO/IEC 19790, 24759 기반의 FIPS 140-3으로 변경하고 있으며, 2020년 9월 22일부터 실제 시험에 적용할 예정이다. 이러한 변화와 더불어 ISO/IEC 19790, 24759의 비침투공격 보안 요구사항에 대한 구체적인 시험 방법, 시험 도구 요구사항, 시험 도구 설정 방식 등에 관한 표준이 ISO/IEC JTC 1/SC 27에 의해 ISO/IEC 17825와 20085-1, 2으로 각각 발간 혹은 표준 제정 진행중에 있다. 본 논문에서는 비침투보안 시험방법론과 관련된 ISO 표준인 ISO/IEC 17825와 20085-1, 2를 통해 비침투공격 시험방법론 표준화 동향에 대해 살펴보고자 한다.

## Ⅰ. 서 론

비침투공격 및 대응방법에 대한 시험은 암호모듈 검증제도와 CC평가 등에서 활발히 이루어지고 있으며, 실제 신용카드, 암호모듈의 안전성 평가에 있어서 중요한 부분을 차지하고 있다. 최근 미국 CMVP 제도는 기존의 FIP140-2 기준에서 ISO/IEC 19790, 24759 기반의 FIPS140-3으로의 기준 변경을 진행하고 있으며, 해당 표준들은 현재 한국 암호모듈 검증제도(KCMVP)에서도 시험 기준으로 사용하고 있다. 이러한 암호모듈 검증에 관한 미국의 기준 변경으로 ISO/IEC 19790, 24759 표준 및 관련 사항의 중요도가 더욱 높아지고 있다. 해당 표준들에서는 암호모듈의 보안 수준별 부채널 공격 대응에 대한 보안 요구사항을 제시하고 있으며, 해당 보안 요구사항에 부합하는 부채널 공격 대응에 대한 시험 방법, 시험 도구 요구사항, 시험 도구 설정과 관련된 부분은 ISO/IEC 17825와 ISO/IEC 20085-1, 2 표준들을 참고하도록 되어있다. 본 논문에서는 부채널 공격 시험 방법, 시험 도구 요구사항, 시험 도구 설정과 관련된 ISO/IEC 17825와 ISO/IEC 20085-1, 2 표준들의 내용과 최신 동향에 대해 살펴보고자 한다.

## Ⅱ. 표준화 동향

본 장에서는 현재 암호모듈 검증 기준인 ISO/IEC 19790, 24759의 보안 수준별 부채널 공격 대응 시험 방법 및 시험 도구/설정 방식에 관한 국제 표준인 ISO/IEC 17825와 20085-1, 2의 내용 및 최신 동향에 대해 살펴본다.

### 2.1. ISO/IEC 17825

ISO/IEC 17825는 암호모듈에 대한 비침투공격 완화를 위한 테스트 방법론에 관한 표준으로 2016년 1월 첫 번째 버전이 발간되었다. 해당 표준은 암호모듈 검증과 관련하여, ISO/IEC 19790:2012에 지정된 보안수준 3, 4에 해당하는 비침투보안 요구사항에 대해 암호모듈의 적합성 여부를 결정하기 위한 테스트 기준을 명시하고 있다. 암호모듈이 ISO/IEC 19790:2012에 명시된 각 보안 요구사항과 연관된 보안 기능들에 대해, ISO/IEC 17825의 테스트 기준을 준수하는지 여부를 시험하기 위한 방법은 ISO/IEC 24759:2014에 명시되어 있다.

ISO/IEC 17825는 ISO/IEC 19790:2012를 준수하기 위해 암호모듈이 대응 기법을 적용해야 하는 비침투 공격 방법과 각 공격 방법에 연관된 보안 기능을 구체적으로 명시하고, 각각의 테스트 방법을 기술하고 있다.

* 한국전자통신연구원 부설 연구소(연구원, thpark@nsr.re.kr, 선임연구원, jhpark84@nsr.re.kr)
** 교신저자, 한국전자통신연구원 부설 연구소(선임 연구원, jsw@nsr.re.kr)

또한, 대칭키 및 비대칭키 암호 시스템의 부채널 분석을 위한 테스트 방법과 ISO/IEC 19790:2012에 대한 적합성을 입증하기 위한 비침투 공격 완화 Pass/Fail 테스트 기준을 지정하였다.

Common Criteria와 같이 비침투 보안을 요구하는 몇몇 인증 프로그램들은 Evaluation 형태의 접근 방법을 사용하여 비침투 보안에 대한 평가를 진행하고 있다. 그러나 Evaluation 형태의 평가 방법은 암호모듈 검증 제도와 같은 Conformance 형태의 평가에는 적합하지 않다. 존재하는 모든 부채널 분석 공격에 대한 안전성을 평가하는 것은 현실적으로 쉽지 않으며, 표준화되지 않은 평가 방법은 암호모듈이 부채널 분석 공격에 저항성을 가지고 있음을 보증하기 어렵다. 또한, 부채널 분석의 특성상 공격자 혹은 평가자의 경험과 능력에 따라 암호모듈의 부채널 분석 결과가 일정하지 않을 뿐만 아니라 결과에 상당히 큰 격차가 발생할 수 있다. 따라서, 효과적이고 비용 효율적인 Conformance 형태의 비침투 평가 방법이 반드시 필요하며, 이를 마련하기 위한 다양한 연구들이 수행되고 있다. ISO/IEC 17825는 이러한 문제점을 어느 정도 보완할 수 있는 비용 효율적인 “Push-button”방식의 테스트 방법을 명세하고 있다.

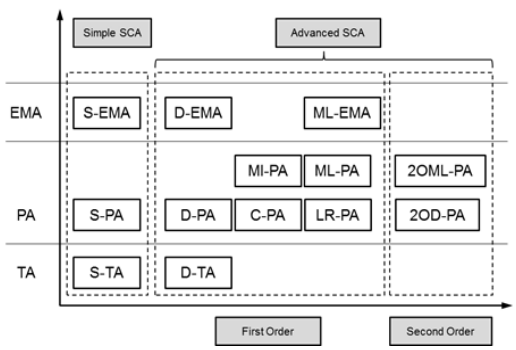
먼저, 비침투 공격에 사용될 수 있는 암호 시스템의 부채널 정보는 크게 3종(소비 전력, 전자기 방출, 연산 시간)의 클래스를 고려하여 그림 1과 같이 분류하였다. 또한 향후 새로운 공격 채널 및 방법이 추가될 수 있는 부채널 정보의 특징을 고려하여, 서로 다른 공격 간의 관계를 강조하고 공격 방법을 형식화하여 표현함으로써 공격의 분류 체계를 정형화 하고자 하였다. 비침투 공격 방법은 암호 시스템의 CSP를 사용하는 특정 보안 기능과 관련이 있으므로, 위와 같이 분류된 비침투 공격 방법과 ISO/IEC 19790:2012의 부속서 C, D, E에 명시된 보안 기능의 연관성을 표 1과 같이 나타냄으로써, 표준이 다루고 있는 비침투 공격의 범위를 명확히 하였다.

〔표 1〕 비침투 공격과 보안 기능의 연관성

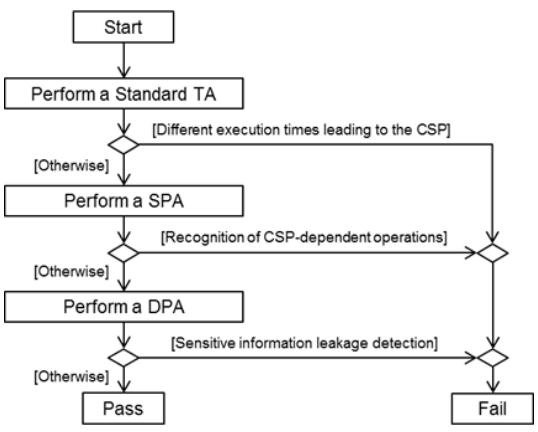
(A: Applicable, NA : Non-Applicable)

| Security Functions | | Attacks Methods | | |
|---|---|---|---|---|
| | | SPA /SEMA | DPA /DEMA | TA |
| Symmetric Key | AES | A | A | A |
| Asymmetric Key | RSA PKCS#1 v1.5 | A | A | A |
| | RSA PKCS#1 v2.1 | NA | NA | A |
| Key Generation | | A | NA | NA |
| Key Entry and Output | | NA | NA | NA |
| … | | … | … | … |

표준에 명세된 부채널 저항성 시험 프레임워크는 그림 2와 같다. 표준에 따라 시험기관은 TA, SPA, DPA에 대한 IUT(Implementation Under Test)의 시험을 수행해야 하며, 프레임워크에 명시된 순서대로 시험을 진행해야 한다. 시험 진행을 위해 벤더가 제공해야 하는 정보와 기능 외에도 시험기관이 수행해야 하는 정보 누수 분석 절차를 각 공격 방법 별로 명세하고 있다. 이러한 일련의 절차를 통해 부채널 저항성 시험의 성공/실패 여부를 결정하게 된다. 이 때, 공격 대상 CSP 전체의 추출 여부가 아니라 중요한 정보의 유출이 존재한다고




〔그림 1〕 비침투 공격 분류




〔그림 2〕 부채널 저항성 시험 프레임워크

판단할 수 있는 근거의 유무에 따라 시험의 결과를 결정하는 방식을 제안하고 있다.

ISO/IEC 17825는 대칭키 및 비대칭키 암호 시스템의 비침투 공격 중 DPA/DEMA에 대해 상당히 자세한 시험 방법을 명세하고 있다. 테스트벡터 기반 정보누수 분석(이하 TVLA) 이라 불리는 이 평가 방법은 2011년 처음 발표되었고, 이후 많은 암호 시스템의 부채널 분석에 대한 안전성 평가 방법으로 연구 및 활용되고 있다 [1, 2]. TVLA는 통계적으로 유의미하게 부채널 정보에 영향을 줄 수 있는 모든 민감한 연산 과정과 그 값은 잠재적으로 취약점을 발생시킬 수 있다는 사실에 근거하여 제안되었으며, 다수의 민감한 중간 연산 및 값 중 부채널 측정 데이터에 큰 영향을 미치는 부분을 탐지하기 위해 통계적 가설 테스트를 사용한다. 수집된 부채널 측정 데이터는 연산 중간값이 다르도록 두 집단으로 분류되는데, 이 때 통계적 가설 테스트에 사용되는 귀무 가설은 두 집단의 부채널 정보 측정값이 동일한 평균과 분산을 갖는다는 것이다. 즉, 중간 연산 및 값이 이러한 평균과 분산에 영향을 미치지 않는다는 것이며, 이에 대한 대립 가설은 두 집단의 평균과 분산이 다르다는 것이다. 통계적 테스트 방법으로 사용되는 Welch T-test는 공격자가 수집할 수 있는 데이터 집합과 비슷한 크기의 데이터 집합이 귀무 가설을 기각하기에 충분한 근거를 제공하는지 여부를 결정한다. 즉, 통계적 테스트는 비침투 보안 평가에 대한 통과/실패의 기준을 설정할 수 있는 신뢰도 점수를 산출한다. TVLA 방법을 사용하면 부채널 수집 정보에서의 정보 누출을 합리적인 시험 시간 내에 감지 및 평가할 수 있으며, 테스트하는 시험자가 최신 부채널 공격에 숙련되어 있지 않아도 평가를 수행할 수 있다. TVLA는 주로 국제 표준 알고리즘인 AES와 RSA 등을 대상으로 한 시험 체계와 방법만이 알려져 있다. 따라서, 만약 이 방법을 국산 암호 알고리즘이나 다른 신규 알고리즘의 부채널 정보 누출 여부를 분석하는데 활용하고자 한다면, 해당 알고리즘의 구조에 따른 적합한 테스트벡터 생성 방법에 대한 연구 및 검토가 요구된다.

비침투 공격 완화 Pass/Fail 시험을 위한 테스트 기준은 데이터 수집 시간 및 분석 시간, 데이터 양을 통해 제공되고 있다. 시간과 관련된 테스트 기준으로 각 개별 시험에 대해 Acquisition Time을 보안수준 3은 최대 6시간, 보안수준 4는 최대 24시간의 제한을 두고 있다. 또한 모든 절차에 대한 Acquisition Time을 보안수준 3은 최대 72시간, 보안수준 4는 최대 288시간으로 제한한다. 부채널 분석에 사용되는 데이터 양과 관련하여 보안수준 3에 해당하는 경우 DPA는 시험 별로 10,000개, TA는 시험 별로 1,000 개의 데이터 셋을 요구한다. 보안수준 4에 해당하는 경우 DPA는 시험 별로 100,000개, TA는 시험 별로 10,000 개의 데이터 셋이 요구된다. ISO/IEC 17825에서는 이러한 테스트 기준을 동시에 적용하여, 어느 한 기준의 제한조건을 충족하면 다른 기준의 조건은 시험 과정에 요구되지 않는다. 그러나 현 표준에서 하나의 기준으로 설정되어 있는 데이터 수집량의 경우, 컴퓨팅 파워의 발전 및 환경에 따라 가변적인 기준이 될 수 있다. 반면 시간에 기반한 기준은 공격자의 능력이나 컴퓨팅 파워의 변동과 관계없는 절대적인 기준이다. 따라서, 다양한 시험 및 연구 데이터를 활용하여 시간에 대한 기준값을 좀 더 면밀히 검토하고, 보안수준에 따른 테스트 기준을 보완 및 개선하는 과정이 필요할 것이라 생각된다.

비침투 공격 완화 평가 방법이 ISO/IEC 17825 표준으로 제정되어 배포되고 있으나, 해당 표준에서 제시하고 있는 비침투 공격 시험 방법은 아직 완성된 기술은 아니다. Carolyn 등은 ISO/IEC 17825에 제시된 방법에 대해 해당 평가 방법의 종합적인 분석 과정 및 검증의 누락과 같은 몇 가지 문제점 및 모호성을 지적하고 개선된 시험 방법 및 기준을 제시하였다[4]. 효과적인 비침투 보안 평가 방법은 대응 기법의 설계 및 구현이 충분히 주의 깊게 모듈에 적용되었음을 평가할 수 있어야 하므로, 비침투 공격 시험에 활용할 수 있는 정형화된 기술에 대한 연구 및 표준화 작업은 암호시스템의 안전성 향상을 위해 지속적으로 보완·발전되어야 할 것이다.

### 2.2. ISO/IEC 20085-1, 2

ISO/IEC 20085-1, 2 [5,6]에서는 앞서 설명한 ISO/IEC 17825에서 언급한 시험 방법론을 지원하기 위한 부채널 공격 시험 도구 요구사항과 시험 도구 조정 방식에 대한 표준 발간에 그 목적을 두고 있다. 현재 ISO/IEC 20085-1은 시험 도구와 기술에 관한 표준으로 2019년에 발간되었다. ISO/IEC 20085-2는 시험 도구 설정 방식과 관련 도구에 대한 것으로 현재 드래프트 상태에 있으며, 발간 예정이다.

ISO/IEC 20085-1에서는 크게 시험 도구와 측정 및 분석 기술로 나누어 기술되어있다. 시험 도구에 관해서는 먼저 부채널 정보의 유형을 소비전력, 전자기파, 연산 수행 시간으로 나누어 정의하였다. 이와 관련하여 부속서 B에서는 부채널 정보 유형에 따른 시험 도구 예시를 제공하고 있다. 시험 도구의 분류는 “Laboratory Assembled”, “Application Specific”으로 나누었으며, 각각의 차이점은 지원하는 부채널 공격 시험 항목이다. 예를 들어, "Application Specific"의 경우, 특정 부채널 공격 시험 목적을 위한 시험 도구라고 할 수 있다. 시험 도구의 구성요소의 경우, 측정 도구, 분석 도구, 시험 도구의 구성 요소별 기능적 항목으로 나누어 아래의 표와 같이 기술되어있다.

〔표 2〕 부채널공격 시험 도구 구성요소 및 기능적 항목

| 구성요소 | 관련 내용 | 기능적 항목 |
|---|---|---|
| 측정 도구 | 부채널 정보 수집 | 프로브<br>증폭기<br>물리적 필터<br>파형 저장<br>파형 조정 도구 |
| 분석 도구 | 1. 측정 과정 제어<br>2. 데이터 후처리<br>3. 후처리 데이터 분석 | 필터링 처리<br>연쇄 분석<br>주파수 분석<br>통계 분석 |

시험 기술 및 관련 접근방식의 경우, 운영 관련, 측정 도구/시험대상, 분석 도구/시험대상, 분석 도구/측정 도구 간의 상호작용에 대해 언급하고 있다. 운영과 관련하여 먼저 수집 유형을 단일 측정과 다중 측정으로 분류를 하였다. 단일 측정은 SPA 테스트와 ISO/IEC 17825, 8.3.2에 언급된 테스트의 두 번째 세트를 위한 것으로 정의하였으며, 다중 측정의 경우, 타이밍 분석, DPA 테스트와 ISO/IEC 17825, 8.3.2에 언급된 테스트의 첫 번째, 세 번째 세트를 위한 것으로 정의하고 있다. 이러한 수집 유형을 바탕으로 수집 과정을 아래의 표와 같이 단계적으로 정의를 하고 있다.

〔표 3〕 부채널 정보 수집 과정

| |
|---|
| Triggering에 따른 정보 수집을 위한 측정 도구 준비 |
| 시험대상으로부터 운영 요청 |
| 데이터 수집 |
| 데이터 저장 |
| 분석 도구로 데이터 전송(임시 저장 혹은 후처리 목적) |

측정과 분석에 있어서 기술적 고려사항은 부속서 A에서 관련 내용을 언급하고 있다. 측정 도구와 시험대상 간의 상호작용과 관련하여 측정 도구에서의 효율적인 대용량 데이터 연속 처리 및 데이터 저장에 관한 내용은 부속서 C에 관련 예제를 제시하고 있다. 분석 도구와 시험대상 간의 상호작용에 대해서는 시험대상으로 입력되는 평문과 출력되는 암호문으로 정의하고 있으며, 분석 도구와 측정 도구 간의 상호작용은 단일 부채널 정보 측정 후 이에 대한 분석이 수행되는 경우 발생한다. 예를 들어, 측정 도구에서 측정된 단일 부채널 정보에 대해 분석 도구에서 데이터 후처리 및 분석이 수행되는 경우가 대표적이다. 이러한 분석 도구와 측정 도구 간 상호작용 발생 시 동기화의 필요성에 대해 언급하고 있다.

ISO/IEC 20085-2에서는 시험 도구 설정 방식, 설정 시 사용되는 신호에 관한 내용에 대해 기술하고 있다. 시험 도구 설정 방식과 관련하여 시험 도구의 정확도의 경우, 샘플링 클럭과 시험대상의 동작 클럭의 동기화가 중요한 것으로 언급하고 있으며, 시험 도구의 정밀도(precision)는 A/D 컨버터의 출력 비트 크기, 샘플링 주기, 주파수의 폭에 의해 결정된다고 언급하고 있다. 시험 도구의 정확도(accuracy)는 앞서 설명한 부분을 기반으로 전압과 시간의 에러, 신호 대 잡음비의 영향을 받는다고 정의를 하고 있다. 시험 도구의 설정은 시험 도구의 정밀도와 정확도를 향상시켜 시험대상이 가지는 부채널 공격 대응기법에 대한 통과/실패 구분을 명확히 하는데 그 목적이 있으며, 서로 다른 시험 도구를 통한 비교 시험을 포함하고 있다. 시험 도구 설정 과정은 2회에 걸쳐서 진행되며, 첫번째는 시험 대상의 보안 수준에 맞춰 ISO/IEC 20085-1을 기반으로 필요한 정보를 충분히 수집 후 분석 수행을 통해 통과/실패를 결정한다. 두 번째 설정과정은 앞선 과정에서 설정한 시험 파라미터를 상향 혹은 하향 조정하여 같은 결과가 도출되는지 확인하는 과정으로 진행된다. 이러한 2회의 설정 과정을 통해 시험대상의 부채널 공격 대응방식에 대한 시험 결과를 도출할 수 있다. 아래의 표는 앞서 설명한 시험 도구 설정 과정에 관한 알고리즘을 나타낸다.

상기의 시험 도구 설정 과정상 M값은 ISO/IEC 17825:2016에서 정의한 보안 수준 3, 4에 따른 수집 파형 개수인 10,000과 100,000을 의미한다. 그리고 설정

〔표 4〕 시험 도구 설정 과정

| 입력: 시험 도구<br>출력: “통과”/“실패” |
| --- |
| 1. 보안 강도를 한계 수치보다 낮게 설정<br>2. 수집된 부채널 파형으로부터 비밀 정보 복구를 위한 파형 개수 m0 설정<br>3. 보안 강도를 한계 수치보다 낮게 설정<br>4. 수집된 부채널 파형으로부터 비밀 정보 복구를 위한 파형 개수 m1 설정<br>5. if m0 〈 M and m1 〉 M:<br>5.1. “통과” 반환<br>6. else:<br>6.1. “실패” 반환 |

과정상 “성공”은 설정이 완료된 것을 의미하며, “실패”는 설정이 완료되지 않은 것을 의미한다. 이러한 시험 도구 설정 과정은 “성공”으로 판정될 때까지 반복 수행이 필요하며, 이러한 설정을 위해 측정 지점과 설정 파라미터는 신호 대 잡음비가 최대가 되도록 조정되어야 한다. 이와 관련하여 해당 표준에서는 키 복구를 위한 신호 대 잡음비와 수집 파형 개수 간의 관계에 대한 설명 및 Virtex-5 FPGA 보드를 기반으로 한 예시를 포함하고 있다. 그리고 시험대상의 설계 정보, 부채널 공격 대응 방법 등의 정보에 대한 제공 유/무에 따라 Open target과 Closed target으로 나누어 정의하고 있다. ISO/IEC 20085-2의 부속서 A에서는 암호 알고리즘별 설정 계량에 관한 내용을 포함하고 있으며, 부속서 B와 C에서는 각각 FPGA (ChipWhisperer를 예시)와 마이크로컨트롤러 상에서의 부채널 정보 관련 구현 예제를 설명하고 있다. 부속서 D에서는 신호 생성기 및 잡음원 명세에 대해 언급하고 있다.

본 절에서는 ISO/IEC 19790에서 정의한 보안 수준별 부채널 공격 대응 요구사항과 ISO/IEC 17825에서 언급한 시험 방법론을 지원하기 위한 부채널 공격 시험 도구 요구사항과 시험 도구 조정 방식에 관한 표준인 ISO/IEC 20085-1, 2에 대해 살펴보았다. 해당 표준에서의 내용은 실제 암호모듈 대상 부채널 공격 대응 시험 시 사용되는 시험 도구 사용 시 고려되고, 실 적용할 수 있을 것으로 판단된다.

## Ⅲ. 결 론

본 논문에서는 부채널 공격 대응에 대한 시험 방법, 시험 도구 요구사항, 시험 도구 설정과 관련 표준인 ISO/IEC 17825와 ISO/IEC 20085-1, 2의 최신 표준화 동향에 대해 살펴보았다. 현재, ISO/IEC 17825와 ISO/IEC 20085-1은 발간되어 부채널 공격 시험 시 활용이 가능하나, ISO/IEC 20085-2는 현재 표준화 진행 중에 있는 상황이다.

현 표준 시험 방법에 대해 여러 가지 이슈들이 발생하는 만큼, 향후에는 이론적 안전성 보증이 가능한 시험 방법 연구가 필요할 것이라 생각된다. CMVP 시험 기준의 FIPS 140-3으로의 전환을 계기로 CC, CMVP, KCMVP 등 다양한 제도에서 ISO/IEC 17825와 20084-1,2에 기반한 비침투보안 시험 케이스가 크게 증가할 것으로 예상된다. 이에 따라 다양한 시험 케이스와 데이터가 축적되면, 비침투보안 시험방법론과 관련 기술 및 표준도 자연스럽게 보완 및 개선될 것이라 예상된다.

## 참 고 문 헌

[1] Goodwill G., Jun B., Jaffe J. and Rohatgi P., “A testing methodology for side-channel resistance validation”, NIST Non-Invasive Attack Testing Workshop, September 2011.

[2] Jaffe J., Rohatgi P. and Witteman M., “Efficient side-channel testing for public key algorithms: RSA case study”, NIST Non-Invasive Attack Testing Workshop, September 2011.

[3] ISO, “Information technology - Security techniques - Testing methods for the mitigation of non-invasive attack classes against cryptographic modules", ISO/IEC 17825, 2015

[4] Carolyn Whitnall and Elisabeth Oswald, “A Critical Analysis of ISO 17825(‘Testing Methods for the Mitigation of Non-invasive Attack Classes Against Cryptographic Modules’), ASIACRYPT 2019, LNCS 11923, pp. 256-284, 2019.

[5] ISO, Information technology - Security techniques - Testing requirements for cryptographic modules", ISO/IEC 24759, 2017

[6] ISO, “IT Security techniques - Test tool requirements and test tool calibration methods

for use in testing non-invasive attack mitigation techniques in cryptographic moudules - Part 1: Test tools and techniques", ISO/IEC 20085-1, 2019

[7] ISO, “IT Security techniques - Test tool requirements and test tool calibration methods for use in testing non-invasive attack mitigation techniques in cryptographic moudules - Part 2: Test calibration methods and apparatus", ISO/IEC DIS 20085-2

## 〈저 자 소 개〉

**박 태 환 (Tae-Hwan, Park)**

정회원

2013년 2월 : 부산대학교 정보컴퓨터공학부 졸업
2019년 2월 : 부산대학교 전기전자컴퓨터공학과 박사
2018년 12월~현재 : 한국전자통신연구원 부설 연구소
<관심분야> 공개키 암호, CMVP, 부채널 공격

**박 진 형 (Jin-Hyung Park)**

정회원

2010년 2월 : 건국대학교 컴퓨터공학과 학사
2019년 2월 : 고려대학교 정보보호대학원 박사
2018년 12월~현재 : 한국전자통신연구원 부설 연구소
<관심분야> Crypto System, CMVP, Data Protection

**장 상 운 (Sang-Woon Jang)**

정회원

2002년 2월 : 고려대학교 수학과 졸업
2004년 2월 : 고려대학교 정보보호대학원 석사
2004년 2월~현재 : 한국전자통신연구원 부설 연구소
<관심분야> 공개키 암호, CMVP, 부채널 공격