"신규 부채널 분석 기술" 특집호 발간에 즈음하여

코로나19 사태로 인한 4차 산업혁명의 가속화로 인해 경제·사회 구조가 급변하는 뉴노멀 시대가 도래하였고, 이러한 변화는 IT자산보호, 정보보호, 제도화에 따른 보안, 위험관리라는 울타리를 쳐서 보호하던 기존 도메인 중심의 전통적 사이버보안을 넘어서서 '보안의 내재화'를 요구하게 되었다. 그리고 '보안의 내재화'에 있어 보안 기반 기술인 '암호기술의 안전성'이 그 무엇보다 강조되고 있는 상황이다.

이러한 상황에서 이론적으로 안전하게 설계된 암호 알고리즘일지라도 알고리즘 구동 시 누출되는 전력/전자파, 소리, 발열량, 캐쉬타이밍 정보 등의 부가정보를 활용하여 실질적으로 암호해독을 가능케 하는 부채널 분석 기술에 대한 연구가 활발히 진행되고 있다. 소형 IC칩부터 고사양 클라우드 서버까지 다양한 제품군에 대한 부채널 분석 사례가 국내외 언론과 문헌 등을 통해 꾸준히 보고됨에 따라, 전 국민이 생활 속에서 보편적으로 사용하는 금융카드, 전자공무원증, 스마트폰, 노트북, PC, 스마트 TV 등에 대한 부채널 분석 안전성 확보와 관련 산업 육성이 절실히 필요한 실정이다. 뿐만 아니라, IT융합무기체계와 드론 등 무인이동 무기체계의 등장으로 인해 군의 암호기술 수준이 한 국가의 국방과 안보수준을 보여주는 핵심지표가 되는 현재 상황에서 부채널 분석에 대한 취약점 검증 기술 및 대응기술 분야의 인력 양성 또한 시급한 상황이다.

본 특집호에서는 부채널 분석에서 활용하는 부가 정보에 따른 분석 및 대응 기술 동향과 신규 분석 기술에 대해서 살펴보았다. 우선 동향 연구와 관련하여 2008년부터 지속적으로 연구되고 있는 RAM 데이터 복구와 관련된 콜드 부트 공격, NIST 후양자암호 공모에 최종 후보로 선정된 격자기반 암호 알고리즘들에 대한 전력/전자파 공격, 시간 공격에 안전성을 제공할 수 있는 Constant Timing 구현 기술 동향에 대해 살펴보았다. 또한, 본 특집호에서는 기존 연구 동향 외에도 신규 부채널 분석 기술을 살펴보았다. 이와 관련하여 무인이동체 환경에서 가장 널리 사용되고 있는 MEMS 센서를 대상으로 신호 오류주입 공격을 재연하고 해당 기술을 탐지하는 방안, 기존 리턴 스택 버퍼를 이용한 마이크로아키텍처 데이터 샘플링 공격의 개선 방안, NIST 후양자암호 전자서명 알고리즘 최종 후보인 FALCON 암호에 대한 부채널 분석 취약 가능성에 대해 살펴보았다.

끝으로 바쁘신 중에도 소중한 시간을 내시어 원고를 집필해 주신 집필자분들과 편집에 수고해 주신 한국정보보호학회 편집위원회, 그리고 학회 사무국 관계자 여러분께 감사를 드립니다.

2021년 2월

고려대학교 인공지능사이버보안학과 **김 희 석**