[정보보호] 경량 암호기술 표준화 추진 현황

IT(Information Technology)가 발전하고, 스마트 기기가 널리 보급됨에 따라 개인정보 등과 같은 중요한 정보를 빠르고 안전하게 저장하고 전송하는 것이 필요하게 되었다. 이를 위해서는 (대칭 키, 비 대칭 키)암호 알고리즘, 해시함수, 전자 서명, 인증 등 여러 가지 암호기술 등이 필요하다. 이러한 암호기술들(cryptography and security mechanisms)에 대해, 국제 표준화 기구/국제 전기 표준화 위원회 합동기술위원회 1 연구그룹 27 작업 그룹 2(ISO/IEC JTC 1/SC 27 WG2, 이하 작업 그룹 2)에서 표준화를 수행하고 있다.

경량 암호기술 소개

국제 표준 문서 ISO/IEC 29192(이하 ISO/IEC 29192)는 경량 암호기술에 대한 표준 문서이다. ISO/IEC 29192에서 첫 번째 파트(ISO/IEC 29192-1)는 경량 암호기술의 정의 등 기본적인 사항이 기술되어 있으며, 나머지 파트들은 보안기능 별로 ISO/IEC 18033(암호 알고리즘에 대한 국제 표준 문서)과 같이 구분되어 있다. ISO/IEC 29192-1에 따르면 경량 암호기술은 제한된 환경에서 구현하기 위해 설계된 암호기술을 말한다. 여기서 제한된 환경이란, 하드웨어 구현 시 제한된 면적 및 적은 전력 소비량, 소프트웨어 구현 시 작은 프로그램 코드 크기나 작은 메모리 크기 등을 의미한다. 이러한 제한된 환경의 예로는 사물인터넷(IoT, Internet of Things)이나 스마트 기기 등이 있다. 요즘 사물인터넷에 대한 관심이 많아지고 스마트 기기의 보급률이 높아짐에 따라, 이러한 환경에서의 보안에 대해 사회적으로 많은 관심이 생겨나고 있다. 이에 따라 경량 암호기술에 대한 관심 및 중요도가 높아지고 있다.

국외 표준화 추진 현황

현재 경량 암호기술과 관련하여 주요 이슈로는, 경량 암호기술에 대한 표준 문서에서 블록에 대한 파트인 ISO/IEC 29192-2에 미국에서 제안한 암호 SIMON과 SPECK을 포함시키는 것에 대한 사항이다.

미국이 주장하는 SIMON과 SPECK의 장점은 유연성(flexibility)과 성능(performance)이다.

SIMON과 SPECK은 ISO/IEC 29192-2에 현재 등재되어 있는 암호 PRESENT, CLEFIA보다 다양한 블록/키 길이(48/96, 64/96, 64/128, 96/96, 96/144, 128/128, 128/192, 128/256)를 지원하기 때문에, 더 많은 환경에서 사용할 수 있다고 주장한다. 또한, 여러 구현 환경(ASIC, FPGA, Microcontroller, X86)에서의 구현 결과를 제시하여, 하드웨어 및 소프트웨어의 성능이 PRESENT, CLEFIA보다 우수함을 강조하고 있다. 하지만 최근 미국 탬파(Tampa)에서 열린 제52회 ISO/IEC 국제 회의(52nd ISO/IEC JTC1 SC27(IT Security Technique))에서 독일과 벨기에의 대표 발언자들은 3가지 반대 이유를 들면서, SIMON과 SPECK의 표준화에 반대하였다. 독일과 벨기에의 3가지 반대 이유는 다음과 같다.

• 48-비트와 같이 짧은 블록 길이를 사용하는 SIMON과 SPECK의 안전성에 대한 의구심

- 독일과 벨기에 측은 짧은 블록 길이를 사용하는 SIMON과 SPECK의 안전성에 의구심을 나타내면서, SIMON과 SPECK의 표준화에 반대하였다. 이에 미국과 영국 측은 SIMON과 SPECK에 대한 사용 가이드라인을 공개하면, SIMON과 SPECK을 안전하게 사용할 수 있을 것이라고 답하였다. 하지만 독일과 벨기에 측에서는 암호기술을 사용할 때 일반적으로 그러한 가이드라인들을 잘 참고하지 않으므로, 가이드라인으로는 SIMON과 SPECK에 대한 안전성을 보장할 수 없다는 의견을 냈다.

• SIMON과 SPECK의 구조에 대해 개선된 분석 방법들의 발견 가능성

- SIMON과 SPECK은 모듈로 덧셈(modulo addition), 배타적 논리합(eXclusive OR), 순환이동(Rotation)으로 이루어진 ARX(Addition, Rotation, XOR) 구조로 구성되어 있다. 독일과 벨기에 측은, 이러한 ARX 구조에 대한 연구가 현재 진행 중이므로 추후 ARX 구조에 대한 개선된 분석 방법들이 발견될 수 있기 때문에, SIMON과 SPECK에 대한 현재의 안전성 마진(security margin)으로는 안전성을 보장할 수 없다는 의견을 냈다.

• SIMON과 SPECK을 설계한 기관(NSA)에 대한 불신

- SIMON과 SPECK을 설계한 기관은 미국 정보기관인 국가안보국(National Security Agency: NSA)이다. 독일과 벨기에 측은 SIMON과 SPECK을 설계한 기관을 신뢰할 수 없다는 이유로 SIMON과 SPECK의 표준화에 반대한다는 의견을 냈고, 미국과 러시아 측은 설계

기관 때문에 표준화를 반대하는 것은 부당하다는 의견을 냈다.

이러한 독일과 벨기에 대표 발언자들의 반대 의견에 따라, SIMON과 SPECK에 대한 분석 자료 혹은 의견들을 더 수집하기로 결정되어 SIMON과 SPECK의 표준화 추진에 진척이 없게 되었다.

국내 표준화 추진 현황

우리나라의 경량 암호기술로는 대칭키 암호 알고리즘인 HIGHT, LEA와 해시함수인 LSH 등이 있다. 이 중 LEA는 2013년 국가보안기술연구소에서 개발하였고, ARX구조로서 32-비트 플랫폼에 최적화 되어 있는 경량 암호기술 알고리즘이다. 그리고 LEA는 스마트그리드 보안, 모바일 기기 보안 등을 위한 소프트웨어 구현 및 사용을 목표로 설계되었다. 특히, ARM과 같은 모바일 환경에서 암호화 속도가 빠르며, 전력소모량이 적다. 현재 ISO/IEC 29192-2에 등재된 암호 알고리즘들은 하드웨어 구현 시 효율이 높은 암호 알고리즘이 대부분이다. 이는 RFID 등 하드웨어 구현이 필요한 환경을 고려한 것이다. 하지만 스마트 기기의 발전 및 사물인터넷 환경을 고려하면, 환경에 따라 소프트웨어의 구현이 더 적합할 수 있다. 소프트웨어 구현의 장점으로는 암호 키 변경이나 암호 알고리즘 변경 등의 유지보수가 용이하다는 점이 있다. 또한, 암호 알고리즘을 라이브러리 형식으로 배포한다면 소프트웨어 개발자가 바로 사용할 수 있다는 장점도 있다. ISO/IEC 29192-5는 하드웨어 구현에 적합한 경량 해시함수와 소프트웨어 구현에 적합한 경량 해시함수를 구분하여 표준화를 진행하고 있다. 이는 ISO/IEC 29192-2에도 소프트웨어에 최적화된 경량 암호 알고리즘이 필요함을 의미한다.

현재까지 공개된 LEA에 대한 안전성 분석 자료들을 살펴보면 LEA는 충분한 안전성 마진(security margin)을 가지고 있음을 확인할 수 있다. 그리고 현재 룩셈부르크(Luxemburg) 대학의 암호연구그룹(CryptoLux)에서 FELICS(Fair Evaluation of Lightweight Cryptographic System)라는 경량암호 성능측정 프레임워크를 제작하고 있다. 이는 3가지 경량 구현 플랫폼(8비트 AVR, 16비트 MSP, 32비트 ARM)에 대하여 2가지 구현 시나리오를 설정하고 각 시나리오 별로 코드를 제출 받아 성능(코드크기, RAM 사용량, 수행시간) 측정한다. FELICS에서 LEA는 키 길이가 128-비트인 블록 암호들 중 3위(시나리오1), 4위(시나리오2)에 랭크 되었으며, 블록 길이가 128-

비트인 블록 암호들 중에서는 LEA가 가장 우수한 성능을 가진다. 여기서 시나리오1은 블록 암호의 운영모드 중 하나인 CBC모드를 이용하여 128-바이트 길이의 평문/암호문을 암호화/복호화하는 상황을 가정한 것이고, 시나리오2는 CTR 모드를 이용하여 128-비트 길이의 평문을 암호화하는 상황을 가정한 것이다. 이를 통해, ISO/IEC 29192-2에 현재 등재되어 있는 암호 PRESENT보다 LEA가 우수한 성능을 가진다는 것을 확인할 수 있다.

이처럼 LEA는 ISO/IEC 29192-2에 필요한 소프트웨어 구현에 적합한 경량 암호기술이며, LEA의 안전성과 성능은 ISO/IEC 29192-2에 현재 등재되어 있는 암호기술들보다 우수하거나 견줄만하다. 따라서 LEA의 우수성과 활용도에 대한 자료를 충분히 준비하고, LEA의 응용 환경 및 장점을 잘 설명한다면 ISO/IEC 29192-2에 등재될 수 있을 것으로 기대된다.

송정환 (한양대학교 교수, camp123@hanyang.ac.kr)