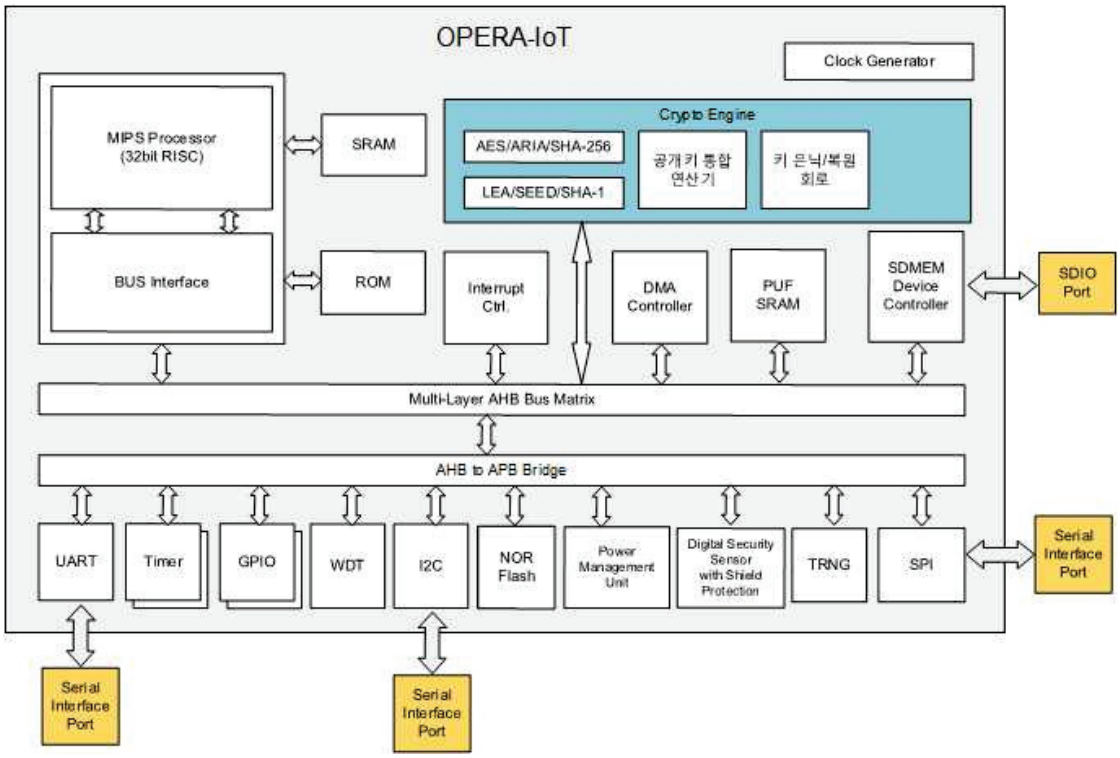
OPERA-IoT 암호칩 제작 및 응용 SW 기술

기술키워드	IoT, 보안칩, 암호칩, OPERA, 사물 인터넷								
지식재산권	출원 1건(미국) / 등록 1건(대한민국)								
기술완성도 (TRL)	기초 실험	개념 정립	기능 및 개념검증	연구실환경 테스트	**시제품 제작**	시제품 성능평가	시제품 신뢰성평가	시제품 인증	상용품

기술개요

- 세부기술[1] - OPERA-IoT 암호칩 제작 기술
  - · OPERA-IoT 암호칩을 제작할 수 있는 통상 실시권
  - · ASIC 제작을 위한 마스크 패턴
  - · 암호칩 데이터 시트 및 매뉴얼
  - · 테스트 프로그램
- 세부기술[2] - OPERA-IoT 암호칩 IP
  - · OPERA-IoT 암호칩에 구현된 암호 및 관련 IP 6종 및 설계서(LEA, SEED, ECC, RSA, PUF, SHA-1)
- 세부기술[3] - OPERA-IoT 암호칩 응용 기술
  - · 암호 IP용 드라이버 및 보안 API
  - · 시험 프로그램

- 기술 구성도



기술성

- IoT 기기 보안 요구 사항을 만족하는 IoT용 암호칩
  - · DPA 대응형 블록 암호 기술(ARIA, LEA, SEED, AES)
  - · 경량에서 고성능까지 모든 응용에 적용 가능한 공개키 기술(응용에 따른 전력·성능 제어)
  - · 확장 가능한 마이크로 코드 기반 공개키 통합 연산기(RSA-1024, 2048, 3072, ECC-224, 256)
  - · SHA-256/SHA-1 지원
  - · 칩의 전영역을 커버하는 Active Shield 기술(칩 내부 탐침방지)
  - · 오류 주입 공격을 탐지하는 디지털 센서 기술
  - · eFuse를 이용한 디버그용 인터페이스 제거 기술
  - · SRAM 기반 PUF 및 키은닉/복원 회로 탑재
  - · TRNG 탑재

시장성

- 최근 통신 3사 및 스타트업 신생 기업을 위주로 IoT와 관련한 서비스 및 제품 들이 등장하고 있으며, 시장이 확대되고 있는 중
  - · 통신 3사에서는 IoT 서비스를 출시하여 서비스 중에 있으며, 그 영역을 확대하고 있는 중
  - · 클라우드 펀딩 등의 투자를 통해 신생 IoT 스타트업이 등장하고 있음
- KCMVP를 만족하는 보안칩은 현재 국내에 없으며, 국내 암호 알고리즘을 탑재하고 있으며, 각종 보호 기술이 탑재된 칩은 OPERA-IoT 칩이 유일함
  - · 해외 유사 제품은 국내 표준 알고리즘을 지원하지 않으며, 가격이 비싼 편임
    - Secusmart Secusuite(독일): €2,500
    - Caspertech Cryptech(이탈리아): €1,700

기술 응용 분야

- IoT 기기 인증 / 기기간 키교환/ 암복호화
- 스마트그리드 보안(스마트미터, DCU, FRTU)

기술개발 완료시기

- 2018년 하반기 완료 예정

관련 특허 등 지식재산권

- (출원) 15/389645(2016. 12. 23. 미국) "데이터 보안을 위한 토글키 차단 방법 및 이를 이용한 장치"
- (등록) 10-1830230(2018. 2. 12. 대한민국) "모듈러 곱셈 장치 및 방법"

기타

- 해당 기술은 3개의 하위 기술로 구분할 수 있으며 각각 기술이전이 가능함(기술이전 상담 시 별도 문의)