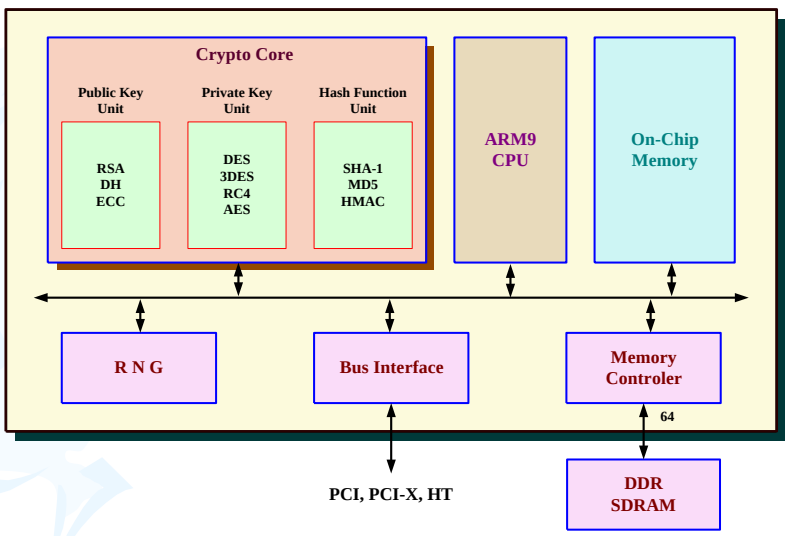
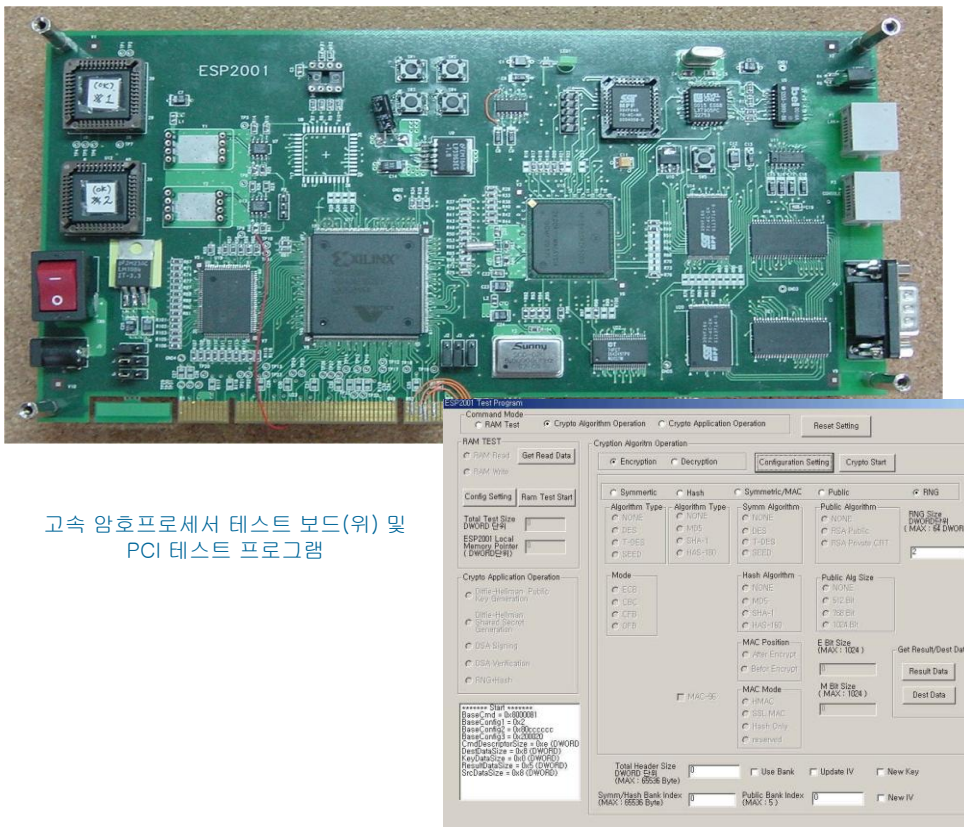
고속 암호화 프로세서 개발

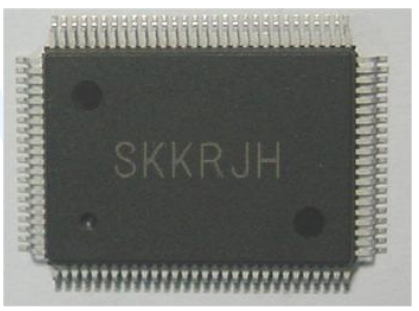
- **과 제 명** : 고속 암호화 프로세서 개발
- **주관기관** : 성균관대학교, 대구대학교
- **위탁기관** : 산업자원부
- **연구기간** : 03. 8.~ '05. 7(2년간)
- **참여인원** : 연구원:9
- **최종제품의 개요** :본 기술개발의 최종 목표는 다양한 정보보호 서비스를 위한 고속 암호프로세서의 개발이다. 이를 위해 5Gbps의 AES, 0.1msec의 지연시간을 가지는 타원곡선 정수 곱셈기, 초당 2,000번의 키를 교환할 수 있는 Diffie-Hellman 키 교환기. 100Mbps의 난수생성기를 개발한다. 또한 본 연구에서 개발한 암호 모듈과 본 연구팀이 이미 개발 완료한 암호모듈(DES, 3DES, SEED, RC4, RSA, MD5, SHA1, HAS160)을 통합하고, 이러한 암호모듈을 효율적으로 제어하기 위하여 ARM9를 내장하는 SOC(System On Chip)의 구현이 최종 제품개발의 목표이다.



고속암호프로세서 전체 구성도



고속 암호프로세서 테스트 보드(위) 및
PCI 테스트 프로그램



대칭키 암호 가속칩

- **주요기능 및 특징 :**
  - 가변 길이를 지원하는 고속 AES 설계
  - 가변 필드 크기를 지원하는 고속 ECC 프로세서 설계
  - DH 키 교환기 설계 기술 난수 생성기 설계
  - 타이밍 공격 방어
  - 전력 공격 방어 기술
  - DH 키 교환기 설계 기술 난수 생성기 설계 기술
  - System-on-Chip 설계 기술(ARM9 + PCI Interface)
  - 리눅스용 드라이버 및 Crypto API 개발

- **기대효과 :**
  - 세계 최고수준의 암호프로세서 개발 및 SoC 산업의 활성화
  - (AES+ECC) 기능을 수행할 수 있는 암호프로세서의 개발을 통한 다수의 특허 획득 가능
  - 네트워크 보안, 전자상거래, 디지털 서명 분야 뿐만 아니라, 스마트카드와 같이 하드웨어 제약조건이 많은 분야에 사용되므로, 그 응용분야는 매우 넓고, 적용분야 또한 다양함
  - 1차년도 사업추진 중에 산업체의 참여로 자연스런 기술 이전이 가능함