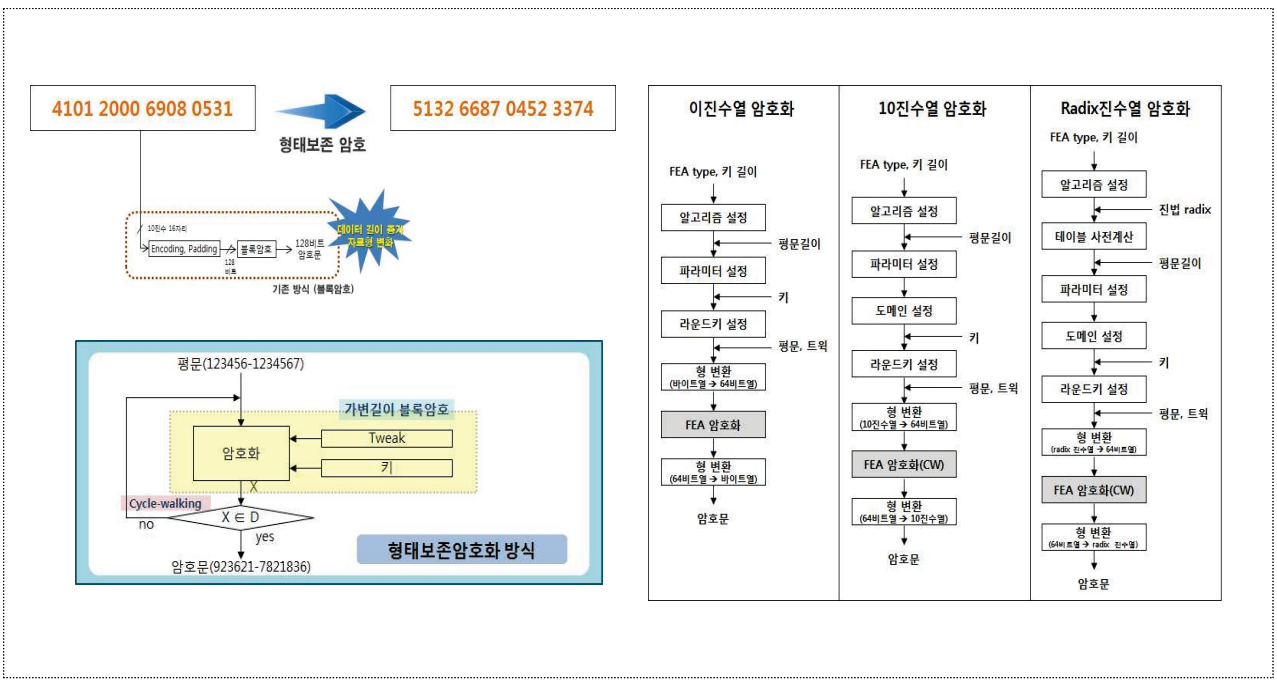
FEA 암호알고리즘을 이용한 형태보존 암호화 기술

기술키워드	DB암호화, 개인정보보호, 형태보존암호화								
지식재산권	-								
기술완성도 (TRL)	기초 실험	개념 정립	기능 및 개념검증	연구실환경 테스트	시제품 제작	시제품 성능평가	시제품 신뢰성평가	**시제품 인증**	상용품

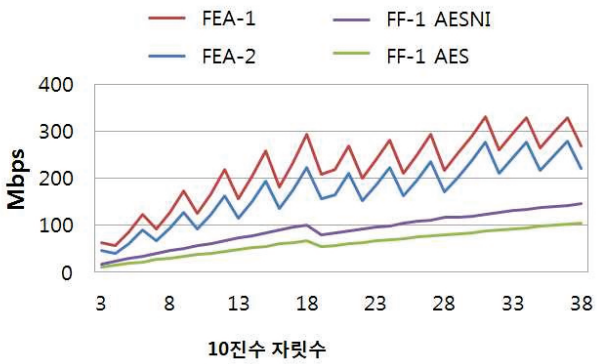
기술개요

- 세부기술[1] - 형태보존 암호화를 위한 형 변환 기술
  - 128 이하의 비트로 표현 가능한 n 자리 radix 진수열을 두 개의 64비트 변수로 변환하거나 그 역 변환을 수행하는 함수의 고속화 기술
- 세부기술[2] - FEA 암호알고리즘 고속구현 기술
  - 8비트 이상 128비트 이하의 임의 길이 비트열을 같은 길이의 비트열로 암호화 하는 FEA 알고리즘을 64비트 환경에서 고속으로 동작하도록 구현하는 기술
  - FEA에 사용된 tweakable feistel 구조의 이론적 안전성이 증명되었음
  - FEA는 tweakable 블록암호의 공격방법에 대해 충분한 안전성을 가진 것으로 분석되었음
- 세부기술[3] - 암호화 기능 구동 기술 및 인코딩 유지 암, 복호화 기능 개발 기술
  - 데이터 형태에 따른 사전계산 및 파라미터 설정으로 효율적인 암호기능 개발 기술
  - FEA를 이용한 ASCII 인코딩 유지 암, 복호화 기능 구현기술
  - FEA를 이용한 유니코드 한글 인코딩 유지 암, 복호화 기능 구현기술
- 기술 구성도



기술성

- 가변길이 블록암호와 Cycle-walking 방식을 융합하여 임의의 도메인에서 암호화 가능하도록 개발
  · 이론적 안전성이 증명된 tweakable Feistel 구조를 기반으로 설계됨
- 형 변환 함수를 최적화하여 암, 복호화를 고속화함
  · 형 변환에 필요한 나눗셈 연산의 횟수를 최소화 하는 기법을 적용
  · 나눗셈 연산을 고속으로 구현하는 기술을 적용함
- 기존 기술(미국 NIST 표준 초안, FF-1) 대비 최고 3배의 성능
  · FF-1은 기반 블록암호를 10회 이상 반복하는 블록암호 운용모드 방식으로 구성됨
  · 블록암호 실행횟수가 많고, 매 반복마다 형 변환 함수를 구동하도록 설계되어 효율성이 떨어짐
  · 본 기술은 비트길이를 보존하는 가변길이 블록암호를 기반으로 하여 연산량이 적음
  · 형 변환 함수가 입력, 출력 시 2회만 구동되므로 효율성이 우수함



시장성

- 2014년의 DB 암호 관련 매출은 64,093백만 원으로 2013년 대비 5.6% 증가였고, 이 중 개인정보를 다루는 공공, 금융, 서비스 분야의 시장점유율은 약 82%임
  ※ 2014 국내 정보보호산업 실태조사 보고서의 DB암호 매출 참조(지식정보보안산업협회 발간)
- 최근까지 지속적으로 발생하고 있는 대형 개인정보유출사고 및 DB 해킹사고로 비추어 볼 때, 데이터베이스 암호화 시장은 지속적으로 성장할 것으로 판단됨
- 클라우드 및 스마트 모바일 환경의 확산으로 데이터베이스의 규모와 보안위협이 동시에 증가 하고 있어 데이터베이스 암호화의 중요성이 더욱 증대될 것으로 판단됨

기술 응용 분야

- 데이터 형태의 유지가 필요한 데이터베이스 등의 암호화 기능 구현에 활용이 가능하며 특히 주민등록번호 등 개인정보의 암호화에 활용이 가능함
- SAP 등 DB 파라미터의 변경이 불가능한 시스템의 암호화에 활용이 가능함
- 동일 형태의 짧은 데이터의 송, 수신이 빈번한 금융관련 통신정보 암호화에 활용이 가능함

기술개발 완료시기

- 2015년 4월 완료

기타

- 해당 기술은 3개의 하위 기술로 구분할 수 있으며 각각 기술이전이 가능함(기술이전 상담 시 별도 문의)
- 3개의 하위 기술은 앞선 기술개요에 세부기술 [1], [2], [3]으로 명시