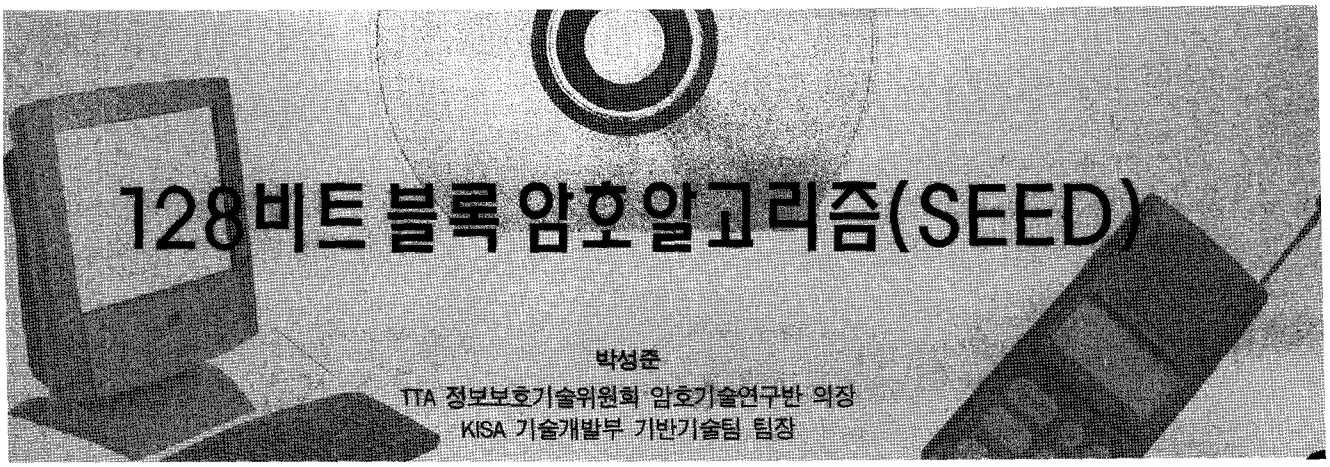

128비트 블록 암호알고리즘(SEED)

박성준
TTA 정보보호기술위원회 암호기술연구반 의장
KISA 기술개발부 기반기술팀 팀장

제1절 개요

국가·사회 정보화 진전과 더불어 다양한 정보통신서비스가 구축됨에 따라 전자상거래, 개인정보 등 민감한 정보를 보호할 수 있는 안전성·신뢰성이 검증된 암호알고리즘의 개발 및 표준화가 요구되어 한국정보보호센터에서는 국내 암호전문가들과 공동으로 128비트 블록암호알고리즘(SEED) 초안을 개발('98. 10.)하고, 공개 검증과정을 거쳐 안전성과 성능이 개선된 최종 수정안을 개발('98. 12.), 완료하였다. 개발된 SEED는 약 4개월여간 공개 검증과정을 거쳐 '99년 2월 26일 최종 개발결과 발표 및 의견수렴을 위한 공청회를 개최하였고 128비트 블록암호알고리즘 표준(안)으로 한국정보통신기술협회(TTA)에 제안하여, 단체표준으로 제정 완료 하였다('99. 9. 28.). 향후에는 국가표준으로 제안할 예정이다.

기본적으로 SEED의 활용분야는 민간분야이다. 민간에서 SEED 사용과 관련해서는 아무런 제약이 없다. 특히, SEED 암호알고리즘 개발목적은 현재 활발히 추진되고 있는 인터넷을 이용한 전자상거래 활성화 촉진을 위해서이므로, 전자상거래에서의 중요 정보를 보호하기 위하여 사용할 수 있다.

한편으로는 SEED 활용을 정부차원에서 촉진하기 위하여는 국가기관에서 사용하는 경우에도, 특수한 경우에 SEED 사용을 허용할 수 있는 방향을 전향적으로 검토하여야 하며, 이를 위해 한국정보보호센터는 국내 암호산업 육성과 연계, 표준제정과 병행하여 관련부처와 긴밀한 협의를 지속적으로 추진하고 있다.

제2절 128비트 블록암호알고리즘 (SEED)

1. 추진 연혁

일시	내용
'97. 9. 1. ~ '98. 9. 1.	128비트 블록암호알고리즘(SEED) 초안개발 완료
'98. 9. 2. ~ '98. 9. 30.	SEED 초안 1차 자체평가 완료
'98. 10. 29. ~ '99. 2. 15.	공개검증을 위한 의견수렴 공고 및 알고리즘 공개
'98. 11. 6. ~ '98. 12. 31.	SEED 공개 검증위원회 구성 및 운영 (4회)
'99. 2. 1.	SEED 수정안 및 분석보고서 공고
'99. 2. 26.	128비트 블록암호알고리즘(SEED) 개발결과 발표 및 활성화를 위한 공청회

일시	내용
'99. 2. 26	소스코드 1차 배포
'99. 3.	TTA표준 제안
'99. 9. 28.	표준 제정(TTA : TTA.KO-12.0004)
~ 현재	소스코드 무상배포 중(90개 기관)

2. 설계 기준

가. 전체구조

- ㅇ 데이터 처리단위 : 8, 16, 32비트 모두 가능
- ㅇ 암·복호화 방식 : 블록 암호방식
- ㅇ 입·출력문의 크기 : 128비트
- ㅇ 입력키의 크기 : 128비트
- ㅇ 안전성 : DC/LC에 대하여 안전하도록 설계.
- ㅇ 구조 : Feistel 구조
- ㅇ 내부함수 : SPN 구조이며, 비선형함수를 Look-up 테이블로 변형하여 사용.
- ㅇ 라운드 수 : 안전성은 키전수 조사공격에 필요한 계산복잡도 및 평문·암호문 쌍(2^{128})이하가 되지 않아야 하며, 효율성 요구조건을 만족하여야 함.
- ㅇ 키생성 알고리즘 : 알고리즘의 라운드 동작과 동시에 암·복호화 라운드 키가 생성될 수 있도록 설계.

나. 안전성에 대한 설계조건

- ㅇ 안전성이 증명 가능한 구조로 설계
- ㅇ 차분해독법(Differential Cryptanalysis, DC)에 대하여 안전하여야 한다.
- ㅇ 선형해독법(Linear Cryptanalysis, LC)에 대하여 안전하여야 한다.
- ㅇ 기타 공격방식(Higher Order DC 등)이 적용되기 어렵게 한다.
  - Higher Order DC에 강하기 위하여 대수적 차수가 3이상인 부울함수를 사용한다.
  - Related Key Attack에 강하기 위하여 Key Schedule에 비선형 함수를 사용한다.

다. 효율성에 대한 설계조건

- ㅇ S/W로 구현시 3중 DES보다 고속이어야 한다.

라. SEED의 일반적 특징

- ㅇ 데이터 처리단위 : 8, 16, 32비트 모두 가능
- ㅇ 암·복호화 방식 : 블록암호방식
- ㅇ 입·출력문의 크기 : 128비트
- ㅇ 입력키의 크기 : 128비트
- ㅇ 라운드 수 : 16라운드
- ㅇ 구조 : Feistel 구조
- ㅇ 내부함수
  - 연산은 ⊞, ⊕만 사용
  - 2개의 안전성이 입증된 S-Box 사용
  - DC, LC에 대한 이론적 안전성 증명 가능
  - 내부함수 F의 구조는 DES, MISTY 등과 비교하여 우수함.

제3절 활용 분야

기본적으로 SEED는 민간분야의 암호사용을 촉진하기 위하여 개발된 암호알고리즘이다. 따라서, 개인 및 기업에서의 중요정보를 보호하기 위하여 필요한 경우 SEED 사용과 관련해서는 아무런 제약이 없다.

가장 대표적인 활용 분야로는 현재 활발히 추진되고 있는 인터넷을 이용한 전자상거래 분야이다. 특히, 전자서명법과 관련하여 1999년 7월 1일부터 공인인증기관의 운영 및 전자서명의 법적 효력이 부여될 예정으로 전자상거래가 매우 활발히 촉진될 것으로 기대된다. 그러나 전자서명법에는 직접적으로 암호사용과 관련한 부분이 없으며, 전자상거래의 안전성·신뢰성 확보를 위해서는 공개키 인증과 더불어 암호사용이 필수적으로 수반되어야 할 것이다. 이 경우 중요 정보의 보호를 위해 표준 암호알고리즘인 SEED를 사용하도록 권고하고 있는 것이다. 구체적인 사용 예로는 전자상거래 이용시

전자거래 내용 및 계좌번호 등의 노출방지를 위한 암호화 등이 있을 것이다. 한편 전자화폐나 전자지불시스템 구현시에도 아무런 제약없이 필요한 데이터 암호화에도 적용이 가능하다. 특히, 현재 진행중인 국내 전자화폐 개발에 SEED가 채용될 것으로 판단된다.

또한 전자상거래외에 대표적인 활용분야는 다음과 같다.

- ㅇ 전자우편시스템에서의 메시지 암호화
- ㅇ PC의 저장된 데이터의 암호화
- ㅇ 가상교육 시스템
  - 유료 수업 내용의 보호
  - 개인별 성적표 내용 등의 보호
- ㅇ 위성방송사업과 연관된 한정수신시스템 (CAS : Conditional Access System)
  - 유료 방송 내용의 암호화

더구나 SEED 활용을 정부차원에서 촉진하기 위해서는 국가기관에서 필요한 경우에도 특수한 경우, SEED 사용을 허용하는 방향으로 검토하여야 한다. 현재 국가기관의 경우 보안업무규정 및 국가전산 보안업무 기본지침에 의해 국가정보원이 주관하고 있다. 그러나 국내 암호산업 육성을 위한 암호산업체의 시장성을 확보하는 차원에서도 국가전산보안업무 기본지침 범위내에서 SEED를 활성화할 수 있는 방법을 전향적으로 강구하여야 할 것이다.

이러한 방법의 일환으로 SEED 적용분야를 일차적으로 민간분야에서 국가기관과 민간분야간의 영역으로 확대하고, 향후에는 국가기관간의 비밀이 아닌 일반 데이터들의 암호통신 영역으로 확대하는 적용분야의 점진적 확대방안이 바람직하다고 생각된다. 이를 위해 한국정보보호센터에서는 SEED 활성화를 통한 국내 암호산업 육성이 원활히 추진되도록 표준제정과 병행하여 관련부처와 긴밀한 협의를 지속적으로 추진할 예정이며, 관련 정부부처에서도 국내 암호산업 육성의 필요성을 충분히 인식하고 있으며 SEED 활성화를 위한 전향적인 검토가 진행중인 것으로 알고 있다.

제4절 결론

128비트 표준 암호알고리즘인 SEED는 정부차원에서 개발한 민간분야의 표준 알고리즘이다. 민간분야의 중요정보 보호, 전자상거래 활성화 촉진 및 국내 암호산업 육성 등 다목적을 지향하여 개발되었다. 이러한 원래의 목적을 달성하기 위해서는 SEED 활성화와 관련하여 각계 각층의 지속적인 관심과 정책추진이 요구되는 것이다.

한국정보보호센터를 중심으로, 정부는 SEED 활성화를 위해 정부차원의 활용분야를 개척하고 적용하여야 한다. 이는 바로 국내 암호산업체의 시장성을 확보하는 차원에서도 매우 중요한 일이라고 생각된다. 이를 위해 한국정보보호센터는 SEED가 국내 암호산업 육성의 밑거름이 되도록 국가기관의 경우에도 필요한 경우에는 사용이 가능하도록 관련 정부부처와 지속적으로 긴밀한 협의를 할 예정이다.

한편 암호산업체들은 많은 관심과 애정을 가지고 SEED가 국내 암호기술 발전의 한 획을 그을 수 있도록 많은 사용 및 SEED를 채용한 암호시스템 개발에 주력하여야 할 것이다.

끝으로 암호산업체, 개인 및 기업, 정부 모두는 SEED 활성화에 많은 관심과 협조를 부탁드립니다.