通信情報保護學會誌
第7卷 第2號, 1997. 6

미국의 표준 암호 개발 동향

이 상 진*, 서 창 호*, 이 대 기*

요 약

최근 미국에서는 그 동안 표준 암호 알고리즘으로 사용한 DES를 폐기하고 후속으로 새로운 블럭 암호를 개발하여 표준으로 채택하려 하고 있다. 본 고에서는 현재까지 이루어진 Advanced Encryption Standard 활동을 개괄적으로 기술하고자 한다. 본 고는 추후 국내의 표준 암호 개발에 대한 활동이 있을 경우 참고 자료가 될 수 있을 것이다.

1. 서론

미국에서는 1977년 DES(Data Encryption Standard)[1]를 미국 연방 표준 암호 알고리즘으로 선정한 후 매 5년마다 재평가를 실시하였는데, 1993년에 실시된 재평가 때 DES를 1998년까지 계속해서 표준 암호로 사용하고, 1998년 이후에는 DES를 더이상 표준 암호로 사용하지 않기로 결정하였다[2]. 이러한 배경 하에서 새로운 표준 암호를 선정하기 위한 기반 작업으로 NIST(National Institute of Standards and Technology)는 '97년 1월 2일에 표준 암호로 선정되기 위한 최소 기본 요건, 평가 기준 및 표준 암호로 제안할 때 갖추어야 하는 제안 요건을 발표하였고, 이에 대한 공개적인 비평을 요청하였다[3]. 공개 비평은 4월 2일까지 총 33건이 접수되었는데 이를 4월 15일 개최된 Developing the Advanced Encryption Standard (DAES) Workshop에서 종합적으로 발표하였다[4]. DAES의 결과를 바탕으로 NIST는 6월 13일에 AES를 공모하는 방안을 발표하였는데 주 내용은 AES로 제안하는데 필요한 제반 문건, 제안 알고리즘의 최소 허용 조건, 평가 기준, 평가 절차 등을 언급하고 있다[5].

NIST에서는 다음과 같은 과정을 거쳐 표준 암호를 선정할 계획이다.

- 표준 암호 공개 모집
- First AES Candidate Conference 개최
- 제안된 암호에 대한 1차 검토 : 6개월 소요 예상
- Second AES Candidate Conference 개최 : 5종 이하의 후보 알고리즘 선정
- 후보 암호 알고리즘에 대하 2차 검토 : 6개월에서 9개월 소요 예상
- Third AES Candidate Conference 개최
- FIPS 초안 공표 및 이에 대한 공개 비평을 3개월간 접수
- 최종안 선정 및 공표

* 한국전자통신연구원

본 고는 DAES의 결과와 공모안에 대한 내용을 소개하고자 한다.

2. AES의 제반 조건

NIST는 '97년 1월 2일 AES 개발을 공표하였다. 이와 함께 표준 암호를 공모하기 위한 준비과정으로 표준 암호가 만족해야 하는 기본 요건을 제시하고, 표준 암호로 제안할 때 갖추어야 하는 제출 요건, 제안된 암호들의 평가 기준을 발표하였다. 그리고 이의 합리성에 대한 공개적인 비평을 구했다. 이를 간략히 소개하면 다음과 같다.

표준 암호의 기본 요건

A.1 AES는 공개적으로 정의되어야 함

A.2 AES는 블럭 암호이어야 함

A.3 AES는 필요할 경우 키의 길이를 증가시킬 수 있는 형태로 설계되어야 함

A.4 AES는 하드웨어와 소프트웨어 모두에 구현될 수 있어야 함

A.5 AES는 자유롭게 사용될 수 있거나 ANSI(American National Standard Institute)의 특허 정책에 적합해야 함

위의 기본 요건을 만족하는 암호들 중 표준 암호로 선정하는 평가 기준은 다음과 같다.

평가 기준

a) 안전도(Security), 즉 암호 분석에 소요되는 노력의 양

b) 계산 속도의 효율성(Computational efficiency)

c) 메모리 요구량(Memory requirements)

d) 하드웨어와 소프트웨어에 대한 적합성(Hardware and software suitability)

e) 단순성(Simplicity)

f) 유연성(Flexibility)

g) 사용 허가 여부(Licensing requirements)

또한 표준 암호로 제안하는 경우 갖추어야 하는 제안 요건은 다음과 같다.

표준 암호 제안 요건

B.1 수식, 표, 알고리즘 구현에 필요한 매개 변수 등을 포함하여 알고리즘 설계 명세가 완벽하게 기술되어야 한다.

B.2 PC로 컴파일이 되는 ANSI C 코드로 구현된 Source와 구현 결과를 제출해야 한다. 제출된 소프트웨어는 메모리 요구량과 소프트웨어 성능 평가에 활용된다.

B.3 하드웨어와 소프트웨어로 구현하였을 때 계산 효율성을 예측하여 기술해야 한다.

B.4 특정한 평문에 대한 암호문의 예가 기술되어야 한다.

B.5 알고리즘 구현에 의하여 발생할 수 있는 특허와 소유권 문제를 기술해야 한다.

B.6 알려진 공격 방법에 대한 분석이 있어야 한다.

B.7 제안하는 암호의 장단점을 기술해야 한다.

NIST는 이상의 기본 요건, 평가 기준, 제안 요건 등을 공표하고 이에 대한 공개적인 비평을 요청하였다.

3. 공개 비평과 NIST의 대응

AES의 제반 요건에 대한 공개 비평을 요청한 결과 총 33건이 접수되었다. NIST는 이에 대한 종합 결과를 4월 15일 개최된 DAES Workshop

에서 발표하였다. 본 절에서는 각각의 비평을 소개하고 이에 대한 NIST의 견해를 기술하고자 한다.

3. 1 AES 기본 요건에 대한 비평

다섯 가지 요건에 대해 각각의 비평과 그에 대한 NIST의 견해는 다음과 같다.

A.1 AES는 공개적으로 정의되어야 함

이에 대한 비평은 AEA(Advanced Encryption Algorithm)의 모든 계산은 명확하게 정의되어야 하며, 모든 분석은 공개되어야 하고, 표 생성을 위한 수학 논리는 공개되어야 하는 것으로 요약된다. NIST의 견해는 대체로 동의하는 편이나, 특별히 비밀로 분류되지 않은 분석(unclassified analysis)을 공개하겠다는 입장을 표명하고 있다.

A.2 AES는 블럭 암호이어야 함

이에 대한 비평은 스트림 암호도 고려하는 것이 타당하며, 응용 환경과 각 사용 방식에 따른 최적의 알고리즘을 선택하는 것이 바람직하다는 것과 블럭 사이즈는 128 비트 혹은 256 비트로 고려하는 것으로 요약된다. DES가 잘 이해되어 사용되고, 현존하는 DES 응용 방식에 호환이 가능하기 위해서는 블럭 암호가 적합하다는 것이 NIST의 견해이며, 블럭 사이즈는 명확하게 제시할 필요가 있음을 인정하였다.

A.3 AES는 필요할 경우 키의 길이를 증가시킬 수 있는 형태로 설계되어야 함

이에 대한 비평은 동의하는 쪽과 키 사이즈가 큰 하나를 사용하는 쪽으로 나누어지며, triple-DES를 표준으로 고려할 필요가 있다는 것으로 요약된다. NIST는 키 사이즈에 대해서는 별도의 주제로 토의할 필요가 있다는 견해이며, AES는 triple-DES에 비해 중요한 이점이 제공되어야 한다는 생각이다.

A.4 AES는 하드웨어와 소프트웨어 모두에 구현될 수 있어야 함

이에 대해서는 모든 알고리즘이 하드웨어와 소프트웨어로 동시에 구현될 수 있으므로 불필요하다는 비평이 있다. NIST는 이 조건을 삽입한 동기로 SKIPJACK과 같이 하드웨어로만 구현된다는 지 혹은 소프트웨어로만 구현되는 제한이 없다는 것을 명확히 하려는 의도였음을 밝혔다.

A.5 AES는 자유롭게 사용될 수 있거나 ANSI의 특허 정책에 적합해야 함

이에 대해서는 대다수가 전세계적으로 자유롭게 사용될 수 있어야 한다는 의견을 냈으며, 로얄티가 있는 알고리즘도 배제하지 말라는 소수 의견도 있다. NIST는 1차적으로 자유롭게 사용할 수 있는 것을 선호하고 2차적으로 평가할 때 자유롭게 사용할 수 있는 방식에 가중치를 준다는 의견이다.

3. 2 평가 기준에 대한 비평

평가 기준으로 제시된 것은 총 여섯 가지인데 이에 대한 비평 및 NIST의 견해는 다음과 같다.

a) 안전도(Security)

이에 대해서는 알고리즘에 사용하는 모든 표는 수학적인 방법에 의해 생성되어야 하며, 비밀리에 감추어진 손쉬운 공격 방법이 없어야 한다는 의견이다. NIST는 표 생성에 대한 타당한 근거의 제시를 선호하며, 알고리즘 제안자는 비도 요인을 기술해야 함을 강조하고 있다. 또한 모든 분석 방법들에 대한 실질적인 공격에 필요한 노력의 정도를 계산할 것이라고 주장한다.

b) 계산 속도의 효율성(Computational efficiency)

이에 대해서는 다양한 의견이 제시되었다. 8비트 프로세서에 최적화 여부, C 대신에 JAVA에 구현, 키 설정 허용 시간의 명시, 최소 계산 속도의 명시, 프로세서 구조에 대한 명시 등을 들 수 있으며, NIST가 테스트 시스템의 규격을 공표해야 한다는 의견도 있었다. NIST의 답변은 8비트 프로세서에 대한 효율성이 주어져야 하며, 키 설정 시간이 짧아야 하고, 특히 triple-DES 보다 효율적이어야 함을 강조했다. 효율성 평가는 little endian processor 상에서 시행될 것이고, 테스트 시스템은 공개적으로 명시하겠다고 하였다.

c) 메모리 요구량(Memory requirements)

이에 대해서는 소프트웨어 구현 코드 사이즈, 효율성과 메모리 요구량의 상관관계, 다양한 프로세서에 따른 검토에 대한 의견이 개진되었고, NIST의 답변은 효율성 대 메모리 요구량은 PC 상에서 구현된 C에 대해서 고려할 예정이며, 암호 제안자가 별도로 다른 플랫폼의 결과를 제시하는 것도 환영하고 있다.

d) 하드웨어와 소프트웨어에 대한 적합성 (Hardware and software suitability)

이에 대해서는 8비트 프로세서에 효율적으로 설계되어야 하는지, 하드웨어의 경우 gate count를 제시하여야 되는지에 대한 의문이 있었는데 NIST는 기본 응용은 워드 사이즈가 큰 프로세서에서 사용되더라도 8비트 프로세서에서 동작할 수 있는 유연성에 가치를 둘 생각이며, 하드웨어의 구현인 경우는 암호 제안자의 능력에 따르는 문제이지만 이에 대해서는 크게 기대하고 있지 않고 있다.

e) 단순성(Simplicity)

단순성의 의미에 대한 의문이 제기되었는데 NIST는 설계의 단순성, 안전도와 설계에 대한 수학적 근거의 단순성, 구현의 용이성을 의미한다고 답변하였다.

f) 유연성(Flexibility)

이에 대해서는 유연성이 무엇을 의미하는지에 대한 질의가 있었고, 표준 입출력 규격(interface)을 정의해야 한다는 의견과 더나아가서 평가의 용이성 및 상호 연동을 증가시키기 위해 블럭 사이즈, 키 사이즈, 라운드 수를 고정해야 한다는 의견이 제시되었으며, 다양한 변이를 허용해야 한다는 의견이 제시되었다. NIST는 유연성이란 다양한 응용을 위한 여러 종류의 플랫폼에 구현가능성을 의미한다고 정의하였으며, 평가를 위한 표준 입출력 규격을 고려할 예정이라고 답변하였다. 또한 알고리즘에 대한 변이는 상호 연동을 떨어뜨리며, 안전도 평가를 어렵게 하는 요인이지만 키 공간에 대해서는 신축적인 입장이다. 한편 블럭 사이즈와 키 사이즈에 대해서는 논의할 필요성이 있으며, 주어진 블럭 사이즈와 키 사이즈에 대해서 라운드 수는 고정하고자 한다는 것이 NIST의 의견이다.

g) 사용 허가 여부(Licensing requirements)

이에 대해서는 기본 요건에서 언급한 내용과 동일하여 생략한다.

3. 3 기본 요건 및 평가 기준에 대한 일반적인 비평

표준 암호의 수명은 20년에서 30년은 되어야 한다는 의견이 있었는데 NIST도 이에 동의하고 있다. 그리고 평가 기준은 안전도, 효율성, 비용으로 요약될 수 있는데 이에 대한 우선 순위에 대한 질의에 NIST는 우선적으로 안전도를 고려하며 효율성과 비용은 똑같은 비중으로 다루어질 것이라고 답변하였다.

한편 제안된 알고리즘들은 수출 제한을 하지 말아야 하며, 알고리즘의 개발은 수출 제한 정책과 독립적으로 이루어져야 한다는 의견이 제시되었는데 수출 정책은 NIST가 제어할 수

없는 영역이며, 수출에 관한 법에 저촉되지 않아야 한다는 것이 NIST의 답변이다.

끝으로 NIST는 AEA가 최소한 triple-DES와 동급의 안전도를 가져야 한다고 재삼 언급하였다.

3. 4 표준 암호 제안 요건에 대한 비평

제안 요건으로 제시된 것은 총 일곱 가지인데 이에 대한 비평 및 NIST의 견해는 다음과 같다.

B.1 수식, 표, 알고리즘 구현에 필요한 매개 변수 등을 포함하여 알고리즘 설계 명세가 완벽하게 기술되어야 한다.

이에 대해서는 비도 요인에 대한 최소 허용값이 명시되어야 하며, 완벽한 설계 사상이 요구되어야만 한다는 의견이 개진되었다. NIST는 키 및 블럭 사이즈를 공개적으로 발표할 것이며, 제안자가 합리적인 설계 사상을 제시하여 주길 바라고 있다.

B.2 PC로 컴파일이 되는 ANSI C 코드로 구현된 Source와 구현 결과를 제출해야 한다. 제출된 소프트웨어는 메모리 요구량과 소프트웨어 성능 평가에 활용된다.

이에 대해서는 최적으로 구현한 것과 참고적으로 구현한 것 둘을 모두 제출해야 하며, 평가를 위해 설정한 환경을 명시하고 제출을 위한 매체를 명시하라는 의견이 제시되었다. 참고적으로 구현한 것은 JAVA 또는 C를 사용하고, 최적 구현은 팬티엄 프로세서, 16MB RAM, WIN95에서 동작하는 IBM PC 호환 기종에 적합하게 ANSI C로 구현한 것을 요구하고 있으며, 제출을 위한 매체는 3.5인치 1.44MB의 플라피 디스켓을 요구하고 있다.

B.3 하드웨어와 소프트웨어로 구현하였을 때 계산 효율성을 예측하여 기술해야 한다.

이에 대해서는 성능 분석표 또는 성능에 대한 합리적인 근거가 포함되어야 한다는 의견이 있었는데, NIST의 답변은 속도와 메모리량 사이의 관계 그래프를 요구하고 있으며, 다양한 플랫폼에 대한 효율성 평가로써 암복호화 시간, 키 설정 시간, 하드웨어에 대한 gate count, 메모리 요구량 등을 포함시킬 것을 요구하고 있다.

B.4 특정한 평문에 대한 암호문의 예가 기술되어야 한다.

이에 대한 의견으로써 키, 입출력에 대한 Monte Carlo의 예가 있어야 하며, 유용한 예들이 있어야 한다는 것이 개진되었다. NIST는 Monte Carlo의 예를 공표할 것이며, 알고리즘을 시행하여 예들을 검증할 것이고 알고리즘의 구현의 정당성을 입증할 평가 방안 제시를 허용할 것이다.

B.5 알고리즘 구현에 의하여 발생할 수 있는 특허와 소유권 문제를 기술해야 한다.

제안자는 미국내의 특허와 국제 특허에 관한 사항을 제출해야 하며, NIST는 특허청과 협조하여 암호에 대한 특허들을 검토해야 한다는 의견이 있었는데, 제안에 포함된 특허권 또는 소유권에 대한 어떠한 정보도 제공되길 희망하며, 법률 문제에 대한 연구가 적절히 수행될 것이라고 NIST는 답변하였다. 또한 최적 구현을 제외한 어떠한 제안도 받아들이지 않을 것으로 판단된다.

B.6 알려진 공격 방법에 대한 분석이 있어야 한다.

이에 대한 의견으로 제안되는 암호는 동치키, 취약키, 보수 특성이 없어야 하며, 제안자는 trap-door가 없는 이유를 설명하고, 공개된 분석 결과를 제시해야 함이 개진되었다. NIST에서는 알려진 취약키, 동치키, 보수 특성에 대한 목록을 제시하고 trap-door가 존재할만한 부분에 대한 수학적 근거를 포함시키고 알고리즘 분석 결과 대한 참고 문헌을 제공할 것을 요망하였다.

B.7 제안하는 암호의 장단점을 기술해야 한다.

이에 대해서는 어떠한 예가 있는 가에 대한 질의가 있었는데, 그 답변으로 효율성과 유연성의 기준을 언급한다든지, 수학적인 정당성을 기술한다든지 즉, 수학적으로 설계된 S-box, 다양한 키 설정 시간, 8비트 프로세서나 PC에 고속 동작 등이 예로 들 수 있음을 언급했다.

4. AES 공모안

DAES 결과를 반영하여 6월 13일 NIST는 AES 공모안을 발표하였는데, 주로 AES로 제안하기 위해 필요한 제반 문건, 제안 알고리즘의 최소 허용 조건, 평가 기준, 평가 절차 등을 언급하고 있다[5].

4. 1 AES로 제안하기 위해 필요한 문건

AES로 제안하기 위해서는 다음의 문건들이 제출되어야 한다.

- 표지
- 알고리즘에 대한 상세 설명과 부수적인 첨부 문건
- Magnetic media
- 지적 소유권에 관한 문건

4. 2 표지에 기술되는 내용

- 제안 알고리즘의 이름
- 제일 제안자의 이름, 전화번호, 팩스 번호, 소속, 주소, e-mail 주소
- 공동 제안자의 이름
- 알고리즘 발명자 또는 개발자의 이름
- 알고리즘 소유자의 이름
- 제안자의 서명
- 별도의 연락처

4. 3 알고리즘 상세 설명과 부수 문건의 내용

알고리즘에 대한 완벽한 설명을 요구하고 있으며, 특히 알고리즘 구성에 필요한 수식, 표, 그림, 변수 등에 대한 상세 설명을 요구하고 있다. 또한 라운드 수, 상수 생성 방법 등에 대한 타당한 근거를 요구하고 있다. 소프트웨어 및 하드웨어로 구현되었을 경우의 알고리즘의 성능에 대해서 기술하여야 하는데, 8비트 프로세서와 NIST의 AES 평가 플랫폼에 대한 성능은 기본적으로 포함되어야 하며, 최소한 다음의 내용을 수행하는데 필요한 clock cycle 수가 기술되어야 한다.

- 1회 암호화
- 1회 복호화
- 키 설정
- 알고리즘 초기화
- 초기화 후의 키 변환

Known Answer Test(KAT)와 Monte Carlo Test(MCT)에 대한 내용이 포함되어야 한다. KAT는 ECB 모드로 알고리즘을 동작시킨 예로 다음의 내용이 포함되어야 한다.

- Variable Key KAT : 평문의 모든 비트가 '0'으로 고정되고, 한 비트만 '1'이면서 다른 비트는 모두 '0'인 키에 대한 암호문
- Variable Plaintext KAT : 키의 모든 비트가 '0'으로 고정되고, 한 비트만 '1'이면서 다른 비트는 모두 '0'인 평문에 대한 암호문
- 암복호화 때의 각 라운드의 출력값

MCT는 별도로 지정하는 4개의 Test의 결과로 두개의 ECB mode Test와 2개의 CBC mode Test로 구성된다.

알고리즘의 예측 강도가 기술되어야 하는데 이에 대한 타당한 근거와 분석된 결과가 포함되어야 하는데, 예를 들면 취약키, 동치키, 보수 특성, 키 선택의 제한 또는 유사한 성질들을 포함하며, 만약에 없다면 그에 대한 설명이 첨부되어야 한다. 또한 trap-door가 존재하지 않음에 대한 수학적인 근거를 제시해야 되며, 분석 결과에 대한 참고문헌이 있으면 함께 제출하여야 한다.

알고리즘의 장단점을 기술해야 한다. 예를 들면 다음과 같은 것이 있다.

- 스트림 암호, Message Authentication Code 생성기, 난수발생기, 해쉬 함수 등으로 구현한 것
- 다양한 환경 하에서의 구현 효율성
- 다양한 입출력, 키 사이즈

4. 4 Magnetic media에 포함되어야 하는 것

알고리즘의 효율성보다는 구현이 잘되었는지를 확인할 목적의 구현 예가 있어야 하는데 *ANSI C*로 작성되어야 하며 KAT와 두 가지 동작 모드로 구현되어야 한다. 제안자의 이름, 알고리즘의 이름 "Reference Implementation"으로 명명된 하나의 디스켓 안에 구현 내용이 수록되어야 한다.

최적으로 구현된 소스 코드가 제출되어야 하는데 JAVA로 작성되어야 하며 ECB, CBC 모드로 동작하여야 한다. "Optimized Implementation"으로 명명된 하나의 디스켓 안에 구현 내용이 수록되어야 한다.

KAT와 MCT에 대응하는 입출력, 키에 대한 데이터가 수록된 디스켓이 제출되어야 하며, MS word로 작성된 문건을 수록한 디스켓도 제출되어야 한다.

4. 5 AES의 최소 허용 조건

- 비밀키 암호이어야 함
- 블럭 암호이어야 함
- 키와 입력의 사이즈가 128-128, 192-192, 256-256 비트로 구현될 수 있어야 함

4. 6 평가 기준

4. 6. 1 안전도

안전도는 평가에서 가장 중요하게 고려될 것이며 다음의 요인으로 판단될 것이다.

- 제안된 알고리즘 사이에 비교된 실질적인 안전도
- 제안자가 주장하는 안전도와 비교된 실질적인 안전도
- 알고리즘의 출력과 입력을 랜덤 치환한 것과의 구별가능성
- 알고리즘 평가 과정에서 야기된 비도 요인

4. 6. 2 비용

- 소유권 : AES로 확정되면 전세계에서 무료로 사용될 수 있도록 할 예정이다.
- 계산 효율성 : 소프트웨어와 하드웨어 모두에 계산 효율성을 평가한다. 일차적으로 소프트웨어의 구현과 입력 및 키 사이즈가 128비트를 대상으로 할 것이며, 이차적으로 하드웨어와 그 외의 입력, 키 사이즈에 대한 효율성을 평가할 것이다.
- 메모리 요구량 : 일차 평가에서는 소프트웨어, 이차 평가에서는 하드웨어의 메모리 요구량을 평가한다.

4. 6. 3 알고리즘 및 구현의 특성

- 유연성 : 다양한 키 및 입력 사이즈 제공 여부, 다양한 응용 환경에 적합 여부
- 구현 적합성 : 하드웨어만을 대상으로 구현되는 알고리즘은 제외하며, firmware로 효율적으로 구현될 수 있으면 부가점을 받을 수 있다.
- 단순성 : 알고리즘 설계 및 안전도의 근거가 단순한지 여부

4. 7 평가 절차

4. 7. 1 개요

알고리즘을 접수한 후 제안 요건에 적합한지를 NIST 내부에서 검토한 후, 이에 대한 내용을 공표한다. 제안자의 설명과 공개 비평의 시작을 알리는 의미에서 "First AES Candidate Conference"를 개최한다. 그 후 공개 비평을 접수하고, 일차 평가를 시행하고, 이로부터 소수의 알고리즘을 선정하여 이차 평가를 시행한다.

일차 평가는 공개적인 평가에 의존하여 시행하고, NIST 자체의 평가는 수행하지 않을 예정이다. 일차 평가 동안에는 알고리즘의 수정 제안은 허용하지 않을 예정이며, 수행 기간은 6개월을 예상하고 그 결과를 "Second AES Candidate Conference"를 개최하여 공표한다.

이차 평가에서는 5종 이하의 후보 알고리즘을 선정하여 평가하는데, NIST 자체 평가, 공개 비평, 그 외 유용한 정보들을 사용할 것이며, 주로 안전도, 효율성, 지적 소유권 문제들을 다룰 것이다. 이차 평가 전에 "Second AES Candidate Conference"에서 야기된 약간의 문제점을 보완하여 수정 제안할 기회를 약 2개월간 제안자들에게 부여하려고 한다. 이차 평가는 6개월 내지 9개월 동안 공개적으로 진행될 것이며, "Third AES Candidate Conference"을 개최하여 그 결과를 공표한다.

4. 7. 2 일차 평가

일차 평가에는 모든 공개적인 비평을 접수할 예정이며 주로 다음과 같은 사항이 검토될 것이다.

- 128비트 블럭 128비트 키에 대해서 집중적으로 검토한다.
- 구현이 제대로 되었는지 KAT와 MCT를 이용하여 검증한다.
- 효율성 테스트를 시행한다.

다음과 같은 표준 장비에 의해 효율성 테스트를 시행한다.

- NIST 평가 플랫폼 : 펜티엄 프로를 탑재하고, 200MHz의 clock speed를 가지며, 64MB RAM, OS가 Windows95인 IBM 호환 PC
- 컴파일러

- Reference implementation : ANSI C 호환 컴파일러
- Optimized implementation : Java native 컴파일러

4. 7. 3 이차 평가

일차 평가 결과 5종 이하의 후보 알고리즘을 선정하고 NIST는 자체 평가를 시행하면서 공개 비평도 함께 수용할 예정이다. 이차 평가는 일차 평가와 동일한 환경에서 시행할 예정이며 다음의 것은 최소한 시행될 것이다.

- 128비트 이외의 키, 입력 블럭에 대해 검토한다.
- 다양한 형태의 효율성 테스트를 시행한다. 특별히 하드웨어의 효율성을 검토하기 위해 Hardware Description Language를 명시하려고 한다.
- 그 외 여러가지 요소가 평가될 것이다.

5. 결론

미국에서 현재 진행되고 있는 표준 암호 개발은 시사하는 바가 많다. 평가 기준에서 안전도를 우선적으로 고려하고 있으며, 알고리즘의 모든 상수에 대한 타당한 근거를 요구하고 있는 점등은 눈여겨 볼만하다. 또한 안전도 이외에 구현의 효율성, 다양한 사용 가능성, 단순성 등에 대한 고려가 복합적으로 이루어지고 있는 것은 표준 암호가 되기 위한 조건으로 안전도만을 고려하는 것은 문제가 있음을 알 수 있다.

미국과 연구 환경이 매우 다른 국내에서 미국과 똑같은 절차에 의거 표준 암호를 개발하는 것은 문제가 있을 것으로 판단되지만 블럭 암호의 입출력 사이즈, 키 사이즈, 동작 속도 등에 관한 추후의 논의는 지속적으로 검토되어야 할 사항이고, 평가 기준에 관한 사항도 되새겨 볼 필요가 있다고 판단된다. 그리고 제안된 암호에 대한 분석 방법 및 결과를 연구하면 분석 기술 발전에 유익한 면이 있을 것으로 판단된다.

참 고 문 헌

[1] National Bureau of Standards, "Data Encryption Standard," FIPS Pub. 46, 1977.

[2] National Institute of Standards and Technology, "Announcing the Data Encryption Standard DES," FIPS Pub. 46-2, 1993.

[3] National Institute of Standards and Technology, "Announcing development of a federal information processing standard for advanced encryption standard," Request for comments, http://www.nist.gov/itl/lab/bullfeb.htm, 1997.

[4] B. Schneier, "Meeting report: Developing the advanced encryption standard workshop," http://www.counterpane.com/report.html, 1997.

[5] National Institute of Standards and Technology, "Draft AES Announcement," http://www.io.com/~ritter/, 1997.6.

□ 著者紹介

이 상 진

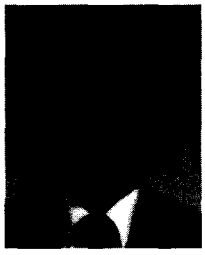
1987년 2월 고려대학교 이과대학 수학과(이학사)
1989년 2월 고려대학교 대학원 수학과(이학석사)
1994년 8월 고려대학교 대학원 수학과(이학박사)
1989년 ~ 현재 한국전자통신연구원 선임연구원

※ 주요관심 분야 : 응용대수학 및 정수론, 암호론

서 창 호

1990년 2월 고려대학교 수학과(이학사)
1992년 8월 고려대학교 대학원 수학과(이학석사)
1996년 8월 고려대학교 대학원 수학과(이학박사)
1996년 ~ 현재 한국전자통신연구원 선임연구원

※ 주요관심분야 : 응용대수학 및 정수론, 암호론



이 대 기

1966년 한양대학교 전공학과(학사)
1987년 한양대학교 전자공학과(석사)
1980년 ~ 현재 한국전자통신연구원 책임기술원

※ 주요관심분야 : 정보시스템 감사, 통제 및 보안