情 報 保 護 學 會 誌
第 12 券 第 3 號, 2002. 6

표준 암호알고리즘 국제 공모사업 동향

천 동 현*, 전 길 수*, 강 성 우*, 현 진 수*, 김 승 주*, 장 청 룡**

요 약

본고에서는 현재 추진중이거나 추진된 표준 암호알고리즘 공모사업에 대한 추진체계 및 현황을 파악한다. 또한 등록방식에서 공모방식으로 전환된 ISO/IEC 국제표준 선정방식의 전환 배경을 살펴보고, 현재 ISO/IEC 국제표준 후보로 제안되어 심의 중에 있는 블록암호 알고리즘 SEED의 표준화 현황을 파악한다.

1. 서 론

암호 알고리즘의 사용이 활성화됨에 따라 선진국들은 자국의 기술력을 대외에 과시하고 정보보호제품의 수출입을 규제하는 등의 목적으로 자국의 표준 암호를 갖고자 많은 노력을 기울이고 있다. 미국의 경우 NIST(National Institute of Standards and Technology)에서 새로운 블록암호 알고리즘 AES(Advanced Encryption Standard)에 대한 공모사업을 주관하여 Rijndael을 표준으로 선정하였으며, 현재는 블록암호 운영모드에 대한 공모사업을 진행 중에 있다. 유럽연합(EU)에서도 회원국들을 위한 암호 알고리즘 공모사업인 NESSIE (New European Schemes for Signatures, Integrity, and Encryption)를 진행하여 다양한 분야의 알고리즘에 대한 표준화를 추진하고 있다. 한편, 일본에서는 2003년 전자정부 구현에 필요한 알고리즘 공모사업으로 CRYPTREC(Cryptography Research & Evaluation Committee)을 진행 중에 있다.

ISO/IEC(International Organization for Standardization/International Electro-technical Commission)는 1999년까지는 암호 알고리즘 등록제로 운영되었으나 2000년 암호 알고리즘에 대하여 공모방식으로 전환되어 현재 국제표준 암호 알고리즘 선정과정에 있다.

본고에서는 이러한 국제적으로 진행되고 있는 표준 공모사업현황에 대해 알아보고, 현재 ISO/IEC 국제표준 블록암호 알고리즘으로 추진되고 있는 SEED의 표준화 현황에 대해 살펴본다.

II. AES

1. 추진배경

대표적인 블록암호 알고리즘인 미국의 DES(Data Encryption Standard)는 1977년 미연방표준 FIPS 46(Federal Information Processing Standard)으로 제정되었다. 이후 NIST에서는 매 5년마다 안전성을 평가하여 향후 5년 간 표준으로서의 적합성 여부를 평가해왔다. 그러나, DES에 대한 다양한 분석기법이 개발되고 컴퓨팅 기술이 발달함에 따라 56비트를 사용하는 DES의 안전성에 문제가 제기되었다. 1993년의 평가에서 처음으로 "DES의 안전성에 대하여 1998년 이후에는 더 높은 안전성을 갖는 대안을 찾아야한다"고 언급되었으며, 이를 보완하는 방법으로 TDES(Triple DES, FIPS 46-3)를 한시적으로 사용하도록 권고되었다.

한편, DES는 NBS(National Bureau of Standards, NIST의 전신)의 주도로 개발된 알고리즘으로, 개발과정 및 설계원칙 등이 공개되지 않았다. 따라서 초기 DES의 키의 크기가 128비트에서 56비트로 축소되고, S-box의 설계원칙이 공개되지 않은 것 등에서 현재까지도 백도어의 존재가능성 여부

* 한국정보보호진흥원 기술단 암호기술팀({dhcheon, kschun, swkang, jshyun, skim}@kisa.or.kr)
** 경동대학교 정보통신공학부(crjang@kyungdong.ac.kr)

가 논란이 되고 있다.

이와 같은 이유로, NIST는 1997년 DES의 후속 표준암호 알고리즘 AES를 정부주도로 개발하지 않고 전 세계를 대상으로 한 공모사업으로 진행하였으며, 평가과정의 투명성을 위해 NIST의 AES 제정을 위한 일련의 활동을 공개하였다[1]. 이를 정리해 보면 다음과 같다.

2. 평가 진행

2.1. AES 공모

NIST는 1997년 1월에 AES 개발 계획을 발표하고, 1997년 4월에 AES 개발 계획과 관련된 워크샵을 개최하여 앞으로의 진행과정에 대한 의견을 수렴하였다. 이후 1997년 9월에 AES 후보 알고리즘 공모를 시작하였으며, 공모는 1998년 6월까지 약 9개월 동안 진행되었다.

- AES의 최소 요구조건
  - 대칭키 블록 암호 알고리즘
  - 128 비트의 블록 크기 지원
  - 128, 192, 256 비트의 가변 키 크기 지원

- AES의 기본 요구조건
  - TDES 이상의 안전성
  - TDES 이상의 효율성
  - 다양한 플랫폼에 적용 가능
  - 지적재산권의 포기

2.2 평가 기준

- 안전성 :
  - 동일한 조건(동일한 키와 블록의 크기)에서 각각의 알고리즘의 안전성 분석
  - 알고리즘의 출력들이 의사난수성을 만족
  - 이론적인 알고리즘의 안전성
  - 실제 평가과정에서 발생 또는 접수되는 의견에서 기인한 가능한 모든 공격에 대한 안전성

- 효율성
  - 하드웨어와 소프트웨어에서의 계산 효율성 (Round 1에서는 키의 길이가 128 비트이고 128 비트 블록인 경우의 소프트웨어, Round 2에서는 다른 키 길이의 소프트웨어와 하드웨어에 대한 평가)
  - 하드웨어와 소프트웨어에서의 메모리 효율성 (Round 1에서는 소프트웨어, Round 2에서는 하드웨어에 대한 평가)

- 알고리즘과 구현 특성
  - 필수 요구조건의 키와 블록의 크기 지원
  - 다양한 플랫폼과 응용프로그램에서 구현가능
  - 알고리즘이 스트림암호, MAC 생성기, 의사난수 생성기, 해쉬 알고리즘으로 응용가능
  - 설계의 명료성

2.3. 평가 일정

2.3.1. AES 서류심사 단계(Pre-Round)

NIST는 1997년 9월에 AES 후보 알고리즘 공모를 시작하면서 알고리즘의 최소 요구 조건, 제출에 필요한 내용, 앞으로의 평가 일정 등을 발표하였다. 이에 따라 1998년 6월까지 9개월 간 진행된 공모에서 AES 후보 알고리즘으로 한국의 CRYPTON, Rainbow를 포함하여 21개의 알고리즘이 접수되었다. 제출된 알고리즘들은 서류심사를 통해 본격적인 Round 1을 위한 후보 알고리즘으로 15개가 선택되었다.

2.3.2. AES 평가 1단계(Round 1)

1998년 8월 20일~22일 미국 캘리포니아 벤추라에서 "First AES Candidate Conference"이 열렸고, 이곳에서 전 세계에서 공모받은 알고리즘 중 AES 평가 준비단계의 서류전형을 거쳐 표 1과 같이 15개의 후보 알고리즘이 발표되었다.

Round 1에서는 블록의 크기 128비트, 키의 크기 128비트인 기본적인 알고리즘의 경우에 대하여 알고리즘의 효율성과 적합성에 중점을 두어 평가하였다.

1999년 3월 22일~23일 이탈리아 로마에서 "Second AES Candidate Conference"가 열렸다. 이곳에서는 15개의 Round 1 후보 알고리즘의 분석 결과와 AES 후보 선정과 관련된 중요한 사항에 대한 논의를 하였다.

〔표 1〕 AES 후보 알고리즘

알고리즘	제 출	제출국
CAST-256	Entrust Technologies, Inc.	미국
CRYPTON	Future Systems, Inc.	대한민국
DEAL	Richard Outerbridge Lars Knudsen	캐나다
DFC	CNRS Ecole Normale Suerieure	프랑스
E2	NTT Corporation	일본
FROG	TecApro International S.A.	미국
HPC	Rich Schroeppel	미국
LOKI97	Lawrie Brown, Josef Pieprzyk, Jennifer Seberry	호주
MAGENTA	Deutche Telekom AG	독일
MARS	IBM	미국
RC6	RSA Laboratories	미국
Rijndael	Joan Daemen Vincent Rijmen	벨기에
SAFER+	Cylink Corporation	미국
Serpent	Ross Anderson, Eli Biham Lars Knudsen	영국
Twofish	Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall, Niels Ferguson	미국

2.3.3. AES 평가 2단계(Round 2)

Round 2에서는 Round 1에서 다룬 기본적인 알고리즘의 경우 이외의 경우에 대하여 알고리즘의 효율성과 적합성을 평가하였으며, 안전성과 관련되어 더 심층적으로 평가하였다.

NIST는 1999년 8월 9일 최종 5개의 후보 알고리즘을 발표하였다[2].

- MARS
- RC6
- Rijndael
- Serpent
- Twofish

2000년 4월 13일~14일 미국 뉴욕에서 "Third AES Candidate Conference"가 열렸으며, Round 1의 평가 과정에 대한 보고 와 Round 1의 평가 결과 및 Round 2의 기술적인 분석에 대한 논의가 있었다.

2.4. AES 평가 결과

2000년 5월 15일 Round 2 평가를 종료한 후, 그동안 분석해온 결과와 전 세계에서 수집된 의견들을 종합하여 2000년 10월 2일 AES로 Rijndael을 최종 선정하였다.

3. 향후 계획

NIST는 AES로 선정된 블록암호 알고리즘에 대한 표준화 추진을 위해 개발한 표준 초안(Draft)을 보완하여 2001년 11월 26일 최종 표준 블록암호 알고리즘 AES(FIPS 197)를 발표하였다[3]. 안전성과 효율성 측면에서 뛰어난 AES는 현재까지 전 세계적으로 널리 사용되었던 DES를 대체하여 향후 폭넓은 분야에서 사용될 것이다.

Ⅲ. NESSIE

1. 추진체계

유럽회원국들은 전자상거래, 전자정부 및 전자서명 등을 실현하기 위해 필수적 요소인 암호 원천기술에 대한 공모사업 NESSIE(New European Schemes for Signatures, Integrity, and Encryption: 2000.1~2002.12) 프로젝트를 추진하고 있다[4]. NESSIE는 전자서명, 무결성 및 암호화 기능을 제공하는 암호 원천기술에 대한 유럽 표준 암호 공모사업으로서 유럽위원회의 정보사회기술 프로그램(IST)의 프로젝트(IST-1999-12324) 중 하나이다.

이 프로젝트의 주요 목적은 투명하고 공개적인 과정을 통해 다양한 플랫폼에 적용 가능한 강력한 암호 원천기술을 개발하는 것이다. NESSIE 프로젝트는 미국의 AES(1997~2000)와 일본의 전자정부 실현을 위한 CRYPTREC(2000~2002) 프로젝트처럼 최고의 암호 전문가들을 중심으로 추진된 민간 주도하의 공모사업이다.

또한 유럽의 정보보호기술에 대한 우수성과 정보보호산업의 활성화 및 높은 우위를 차지하는데 있다. 이 프로젝트는 EU회원국 7개국(벨기에, 프랑스, 영국, 독일, 이스라엘, 벨기에, 노르웨이)의 여러 기관이 참여하고 있다.

2. 평가 진행

2.1 원천기술 공모

NESSIE는 AES와는 달리 다양한 암호 원천기술에 대한 공모사업으로서, 하나의 암호 원천기술을 선정하는 것이 아니라 한 분야에 대해 여러 개의 알고리즘을 선택한다는 것이 특징이다.

〔표 2〕 NESSIE 후보 암호알고리즘

종류		알고리즘 명	제출국
블록암호	64비트	· CS-Cipher · Hierocrypt-L1 · IDEA · Khazad · MISTY1 · Nimbus	프랑스 일본 스위스 브라질 일본 브라질
	128비트	· Anubis · Camellia · Grand Cru · Hierocrypt-3 · Noekeon · Q · SC2000	브라질 일본 벨기에 일본 벨기에 미국 일본
	160비트	· SHACAL	프랑스
	가변길이	· NUSH(64,128,256) · RC6 (128이상) · SAFER++(64,128)	러시아 스웨덴 미국
MAC		· Two-Track-MAC · UMAC	벨기에 캐나다
해쉬함수		· Whirlpool	브라질

2000년 3월부터 2001년 6월까지 암호 원천기술에 대한 공모를 실시하였으며 총 39개(7개의 블록암호, 6개의 스트림암호, 1개의 해쉬함수, 2개의 MAC, 5개의 공개키암호, 7개의 전자서명 기법과 1개의 사용자인증)의 암호 원천기술이 제안되었다. 제안된 알고리즘은 표 2와 같다.

2.2 원천기술 평가

NESSIE에 제안된 암호 원천기술에 대한 평가는 안전성, 시장요구조건, 효율성, 유연성 등의 요구사항을 만족하는지에 따라 이루어진다. 안전성은 발생할 수 있는 기존에 잘 알려진 공격방법에 대해 충분히 안전해야하고 효율성은 메모리와 구현환경에 적합해야한다. 세부적인 요구사항에 대한 내용은 다음과 같다.

- 안전성
  - 가장 일반적인 공격방법인 전수조사, 생일공격 등이 최상의 공격방법이어야 함
  - Timing attack, Power analysis 등과 같은 분석도 고려되어야함
  - 제출자에 의해 제시된 안전성 분석에 대한 객관적인 검정을 통한 평가
  - 난수통계테스트를 만족하여야함

- 효율성
  - S/W및 H/W 구현의 효율성
  - 코드와 메모리의 분야에 대한 적합성

- 기타사항
  - 단순하고 명확한 설계원칙
  - 특허(royalty-free) 및 지적 재산권에 대한 언급 필요

〔표 3〕 NESSIE의 세부일정

일정	내용
2000.01	NESSIE 프로젝트 시작
2000.03	암호 원천기술 공모(3월~9월)
2000.11	1차 NESSIE 워크샵
2001.09	2차 NESSIE 워크샵
2002.02	1차 선정
2002.10	3차 NESSIE 워크샵
2002.12	최종 선정

2.2.1 평가 일정

NESSIE의 모든 평가진행은 공개적인 절차를 통해 이루어지고 있으며 제출된 암호 원천기술과 평가진행에 대한 코멘트를 받아들이기 위해 세 번의 워크샵을 개최하고 있다. 현재까지 1,2차 워크샵을 통해 1차 평가를 하였으며 2002년에 3차 워크샵을 통해 2차 평가를 하여 암호 원천기술에 대한 최종 선정을 할 것이다. NESSIE 프로젝트의 세부일정은 표 3과 같다.

〔표 4〕 1차 평가결과 후보 알고리즘

구분	알고리즘
블록암호	· IDEA · MISTY1 · SAFER++ · RC6 · Khazad · Camellia · SHACAL
스트림암호	· SOBERSNOW · BMGL
MAC, 해쉬함수	· Two-Track MAC · UMAC · Whirlpool
공개키암호	· ACE Encrypt · ECIES · EPOC · PSEC · RSA-OAEP
전자서명, 사용자인증	· ECDSA · ESIGN · QUARTZ · RSA-PSS · SFLASH · GPS

2.2.2 평가 결과

블록암호 알고리즘에 대한 안전성 평가로는 기본적인 키 전수조사(Exhaustive Key Search)와 차분분석(Differential Cryptanalysis), 고계차분분석(Higher Order Differential Cryptanalysis), 부정차분분석(Truncated Differential Cryptanalysis), 불능차분분석(Impossible Differential Cryptanalysis) 등을 고려하여 평가하였다. 또한 선형분석(Linear Cryptanalysis), 대수적 특성(Algebraic Property), 키 관련 공격(Related Key Attack) 등에 대한 분석과 설계자의 안전성 분석결과에 대한 평가를 하였다.

효율성에 대한 평가는 스마트 카드, 일반 PC, 64 비트 처리 프로세스 및 H/W 적용 등의 동일한 플랫폼 상에서 테스트를 실시하였다.

3. 향후 계획

NESSIE는 2002년 11월까지 암호 원천기술에 대한 모든 코멘트를 받아들여 최종 암호알고리즘을 2002년 12월에 선택할 것이다. 이렇게 선정된 암호 원천기술은 무선통신, PDA, 그리고 스마트 카드와 같은 폭넓은 분야에 적극적으로 활용됨으로써 유럽의 전자 정보보호산업의 활성화를 만들 것이라고 보여진다. 또한 선택된 암호 원천기술은 유럽 전자서명 표준(EESSI)을 지원할 것이고 유럽뿐 아니라 전 세계적으로 영향력이 클 것으로 보여진다. 또한 선택된 암호 원천기술은 ISO, IETF 및 IEEE와 같은 표준화로 추진할 것이다.

Ⅳ. CRYPTREC

1. 추진 체계

CRYPTREC(Cryptography Research & Evaluation Committee)은 2003년까지 일본의 전자정부 구축을 위해 구성된 암호기술 평가위원회이다.

일본정부는 전자정부의 구성요소로서 유용하게 이용될 각종 암호기술의 공모를 2000년 6월부터 시작하였고, 응모된 암호기술의 객관적인 평가를 위해 정보기술진흥위원회(IPA, Information-Technology Promotion Agency) 산하에 일본 내의 최고 수준의 암호전문가로 구성된 암호기술 평가 위원회 CRYPTREC을 조직하였다.

이 사업은 일본의 전자정부 구축을 위해 이용 가능한 암호기술에 대한 목록을 작성하여 이에 대한 안전성, 구현성 등의 특징을 기술하는 것이 목적이다. 이를 위하여 평가결과를 포함한 보고서는 IPA 홈페이지(www. ipa.go.jp/security/)에 공고하여 공평성과 투명성을 확보한다.

2. 평가 진행

평가대상 암호기술은 2003년 구축 예정인 전자정부에 적용할 수 있다고 판단되는 암호기술 중에서 공모를 통한 다양한 암호기술 외에 위원회에서 평가가 필요하다고 인정한 암호기술에 대하여 평가가 실시된다. 또한, 각 분야별 소위원회를 설치하여 암호기술 평가의 외부 위탁이나 평가기준 등의 평가 실시방법 및 평가 결과를 검토하여 암호기술 평가위원회에 자문한다.

2.1 암호기술 공모

암호기술의 공모는 총 2 회에 걸쳐 공개키암호, 대칭키암호, 해쉬함수 및 의사난수생성기 등으로 분류하여 공모하였다. 그 중에서 공개키암호는 인증,

서명, 키공유 등으로 분류했고, 대칭키암호는 블록암호와 스트림암호로 분류하였다. 2000년 6월 13일부터 7월 14일까지 진행된 1차 공모 결과 24개의 공개키암호, 19개의 대칭키암호, 5개의 의사난수생성기가 제안되었고, 2001년 8월 1일부터 9월 27일까지 진행된 2차 공모에서는 총 12개의 암호기술이 제안되었다.

2000년에 공모한 암호기술 중 1차 평가[5]를 통과하여 2차 평가 대상이 되었던 알고리즘과 2001년에 새롭게 제안된 암호기술은 표 5와 같다.

2.2 암호기술 평가

CRYPTREC 위원회는 공모된 암호기술 중에서 일본의 전자정부에 필요하다고 생각되는 암호기술을 정리하여 재평가 또는 계속평가를 실시한다.

2001년도에는 신규 응모된 암호기술에 대한 일반평가와 2000년도에 1차 평가를 실시한 암호기술 중 전자정부 암호기술 후보라고 판단된 암호기술에 대하여 계속 평가를 실시하였다[6].

(1) 일반평가

- 서류심사 : 1차 평가로서 제출된 응모서류에 근거하여 암호기술의 문제점을 조사하고 상세평가 수행여부를 결정한다.
- 상세평가 : 안전성 및 성능에 대하여 세부적으로 조사한다. 안전성 평가는 국내외의 암호연구자에게 위탁하여 기존의 분석기술에 대한 평가와 암호기술에 따라 적용 가능한 여러 공격에 대해 평가한다. 또한, S/W 및 H/W에 대한 성능 평가도 수행한다.

(2) 특정평가

ISO/IEC SC27 과 같은 외부기관의 요청 등이나 평가위원회에서 좀 더 상세한 평가가 필요하다고 판단한 암호기술에 대해 특정평가를 실시한다.

〔표 5〕 CRYPTREC에 공모된 암호기술

종류	알고리즘	
대칭키 암호	64비트 블록암호	CIPHERUNICORN-E, FEAL-NX, Hierocrypt-L1, MISTY1, Triple DES**
	128비트 블록암호	Camellia, CIPHERUNICORN-A, Hierocrypt-3, MARS, RC6, SC2000, AES**
	스트림 암호	MULTI-S01, TOYOCRYPT-HS1, C4-1*, FSAngo*, MUGI*
공개키 암호	비밀성	ACE Encrypt, ECAES in SEC1, EPOC, HIME-2, PSEC, HIME(R)*, NTRU*, RSA OAEP**
	인증	ESIGN-identification
	서명	ACE Sign, ECDSA in SEC1, ESIGN-signatures, MY-ELLTY ECMR-h, OK-ECDSA*, DSA**, RSA PSS**
	키공유	ECDHS in SEC1, ECMQVS in SEC1, HDEF-ECDH, HIME-1, Common private Complex Key System*, OK-ECDH*, DH Key Exchange**
해쉬 함수	MD5**, RIPEMD-160**,SHA-1**	
의사 난수 생성기	TOYOCRYPT-HR1, Creation of intrinsic random numbers with Clutter Box*, FSRansu*, High security ultra mini random number generator*, TAO TIME Cognition Algorithm*, PRNG based on SHA-1**	

* 2001년 공모된 암호기술

** 제출된 암호기술 외에 위원회에서 평가가 필요하다고 인정된 암호기술로서 1차 평가를 통과한 암호기술과 함께 상세평가를 실시함.

※ 응모된 암호기술 중 RC6(미국)을 제외한 암호기술은 모두 일본에서 제안되었거나 일본과 공동으로 제안됨.

2.2.1 CRYPTREC 일정

현재까지 진행된 공모 및 평가일정은 〔표 6〕과 같다.

〔표 6〕 CRYPTREC 일정

일시	내용
2000.6.13~7.14	암호기술 공모
2000.7	평가기준 공개
2000.8~9	적격평가 실시
2000.10~12	상세평가 실시
2001.4.18	CRYPTREC Report 2000
2001.8.1~9.27	암호기술 공모
2001.10	응모암호기술 설명회
2001.8~2002.1	적격평가 및 계속평가
2002.1	암호기술 평가 워크샵
2002.4.16	CRYPTREC Report 2001

2.2.2 평가결과

현재까지 진행된 평가 중에서 블록암호알고리즘에 대한 안전성 및 효율성 평가 결과를 살펴본다.

○ 64비트 블록암호

Hierocrypt-L1, MISTY1은 현재까지 안전성에는 문제가 없고, 처리 속도도 빠른 알고리즘으로 분석되었고, CIPHERUNICORN-E, Triple DES는 안전성에는 문제가 없으나 속도가 느리고, FEAL-32X는 장기적인 사용에서는 추천하지 않는다는 평가를 내렸다.

○ 128비트 블록암호

제안된 알고리즘 모두가 현재까지는 안전성에 대해 특별한 문제가 없다고 평가되었다. 다만, RC6는 S/W 처리 속도가 구현된 플랫폼에 크게 의존하고, CIPHERUNICORN-A는 계속 평가가 필요하며 속도가 느린 알고리즘으로 평가되었다.

또한 KISA가 개발한 SEED도 특정평가 대상에 포함되어 평가되었다. 평가 결과 안전성 측면에는 특별한 결함이나 문제점이 발견되지 않는다고 평가되었으나 효율성 측면에서는 속도가 다소 떨어지는 것으로 나타났다.

2.3 향후 계획

이 사업은 전년도와 마찬가지로 신규 공모 및 지속적인 상세평가를 진행하여 2003년 3월 종료된다. CRYPTREC에서 제시되는 여러 암호기술은 일본의 전자정부에 있어 암호 기술을 이용할 때의 참고자료로서 정부 내에서 다양한 형태로 이용될 것으로 예상되고, 기반 기술인 암호기술의 객관적인 평가나 표준화에 적지 않은 기여를 할 것으로 기대된다.

V. SEED의 ISO/IEC 국제표준화 현황

1999년 상반기까지 ISO/IEC JTC 1에서는 비밀성을 보장하기 위한 표준암호 알고리즘을 제정할 때 특정 알고리즘을 선정하여 표준으로 제정하기보다는 등록절차 자체를 표준화(ISO/IEC 9979, 1991(제정), 1999(개정))하여 이에 따라 등록된 암호알고리즘은 모두 표준암호 알고리즘으로 인정하였다. 때문에 회원국들로부터 등록된 암호 알고리즘이 2000년 4월까지 22개에 이르고 어떤 알고리즘이든 등록절차에 따라 등록만 하면 표준으로 인정받는 등 사실상 국제표준으로서의 의미가 유명무실해졌다.

더구나, 암호기술 선진국들은 21세기에 자국에서 사용할 암호 알고리즘을 공모방식으로 선정하여 알고리즘에 대한 안전성을 객관적으로 인정받고 있으며 널리 사용될 것으로 기대되고 있다. 미국에서 추진된 블록암호 알고리즘 공모사업 AES와 유럽 연합에서 추진중인 NESSIE가 대표적인 사례이다.

이에 ISO/IEC는 1999년 ISO/IEC JTC 1/SC 27 전체회의에서 암호 알고리즘 표준제정을 공모방식으로 전환하기로 결정하고 회원국들로부터 후보 알고리즘을 제안하도록 요청하였다. 이러한 요청에 따라 회원국들은 후보 알고리즘을 제안하였으나, 2000년 4월 런던회의에서 후보 알고리즘들에 대한 논의과정 중 제안 지침의 모호성, 제출 기간의 촉박함 등의 문제가 제기되어 수정된 제안 지침[7]에 의거하여 2000년 9월 15일까지 회원국들로부터 공개키, 블록암호, 스트림암호에 대한 후보 알고리즘의 제안을 받아서 2000년 10월 동경회의에서 공개키암호 7개, 블록암호 15개, 스트림암호 1개를 최종 제안하였다. 제안된 알고리즘 및 제안국은 표 7과 같다.

이후 2001년 4월에 개최된 오슬로회의에서 한국은 블록암호알고리즘 ZODIAC을 안전성의 이유로 후보 알고리즘에서 철회하였으며, 미국도 5개의 제안 알고리즘 중 Rijndael(AES)만을 남기고 나머지는 철회하였다. 다만, 다른 회원국으로부터 중복

제안된 RC6과 MARS는 그대로 후보 알고리즘으로 두기로 하였다.

〔표 7〕 ISO/IEC JTC 1/SC27 표준 알고리즘 후보

구분	알고리즘	제안국
블록암호	CAST-128	캐나다
	SEED	대한민국
	XENON	
	ZODIAC	
	AES(Rijndael)	미국
	Serpent	
	Twofish	
	MARS	미국, 일본
	RC6	미국, 스웨덴
	IDEA	스위스
	CIPHERUNICORN-A	일본
	MISTY1	
	Hierocrypt-L1,3	
	Camellia	
공개키암호	ACE	독일
	ECIES	미국
	RSA-OAEP	미국, 스웨덴
	EPOC	일본
	PSEC	
	HIME-1,2	
스트림암호	MULTI-S01	일본

2001년 10월에 개최된 서울회의에서 일본은 CRYPTREC의 평가결과로서 64비트인 블록암호인 MISTY1과 128비트 블록암호인 Camellia만 남기고 나머지 블록암호 알고리즘은 모두 철회하였다. 또한 일본에서 XENON에 대한 이론적 공격가능성을 제시하여 한국은 XENON을 후보 알고리즘에서 철회하였다. 서울회의 결과[8] 작업문서 18033-1의 A.1 선택기준에 맞는 후보인 TDES, MISTY1, AES, SEED, Camellia, CAST-128, IDEA, RC6을 3차 작업문서에 포함시키기로 하였다.

2002년 4월에 개최된 베를린 회의에서 벨기에와 독일은 SEED에 대한 공인된 외부 평가결과의 부족으로 표준안에서의 배제하자는 의견 제시하였으나, 이에 대해 한국은 제 3국의 평가결과인 SEED에 대한 CRYPTREC의 안전성 및 효율성 평가결과[9]를 회의현장에서 제출하였다. 또한 벨기에는 Khazad (64비트 블록암호, 벨기에 및 브라질 공동 개발)를 현 작업문서에 추가하자는 의견을 제시하였으나, Khazad에 대한 NESSIE의 평가결과를 다음 회의인 2002년 10월 바르샤바회의까지 알 수 있으므로 다음 회의에서 논의하기로 하였다. 베를린회의 결과[10] 3차 작업문서에 수용된 블록암호알고리즘 TDEA, MYSTY1, AES, Camellia, SEED, RC6을 모두 4차 작업문서에 포함시키기로 하였으며, 4차 작업문서에 대한 코멘트를 받아 다음회의에서 논의하기로 하였다. 그리고 블록암호알고리즘과 공개키 암호알고리즘에 대한 NESSIE와 CRYPTREC의 평가결과 요약보고서를 2002년 9월말까지 받아 다음 바르샤바 회의에서 발표토록 의뢰하였다.

2002년 10월에 개최되는 바르샤바회의 전까지 블록암호알고리즘들에 대한 최종 평가결과가 나오므로, 바르샤바회의에서 SEED의 1차 위원회문서(CD)로의 포함여부가 최종 결정될 것으로 예상된다.

Ⅵ. 결 론

본고에서는 현재까지 추진중이거나 추진된 표준 암호알고리즘 공모사업인 AES, NESSIE 및 CRYPTREC의 추진체계, 평가과정 및 향후 추진계획 등에 대해 살펴보았다. 또한 등록제에서 공모제로 전환된 ISO/IEC 국제표준에 제안된 SEED의 국제표준화 현황에 대해 살펴보았다. SEED는 다음 바르샤바회의에서 1차 위원회문서(CD)로의 포함여부가 결정될 것으로 예상되므로, 국내 암호전문가들의 작업문서에 대한 적극적인 코멘트 및 관심이 요구된다.

참 고 문 헌

〔1〕 NIST, http://www.nist.gov/aes.
〔2〕 "Report on the Development of the Advanced Encryption Standard (AES)", http://csrc.nist.gov/encryption/aes/round2/r2report.pdf.
〔3〕 FIPS-197 : Advanced Encryption Standard, http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.
〔4〕 http://www.cosic.esat.kuleuven.ac.be/nessie/.
〔5〕 CRYPTREC REPORT 2000, 情報處理振

興事業協會, 2001. 4.
http://www.ipa.go.jp/security/fy12/report/cryptrec- report2k.pdf.
[6] CRYPTREC REPORT 2001, 情報處理振興事業協會, 2002. 4.
http://www.ipa.go.jp/security/fy13/report/cryptrec/c01.pdf.
[7] ISO/IEC JTC 1/SC 27, "Call for contributions on NP 18033 : Encryption algorithms", ISO/IEC JTC 1/SC 27 N2563, 2000.
[8] ISO/IEC JTC 1/SC 27, "Resolutions of the 23rd SC 27/WG 2 meeting in Seoul", ISO/IEC JTC 1/SC 27 N3071, 2001.
[9] ISO/IEC JTC 1/SC 27, "Third Party Evaluation on SEED by CRYPTREC", ISO/IEC JTC 1/SC 27 N3213, 2002.
[10] ISO/IEC JTC 1/SC 27, "Resolution of the 24th SC 27/WG 2 meeting in Berlin, Germany 22nd-26th April 2002", ISO/IEC JTC 1/SC 27 N3186, 2002.

〈著者紹介〉

천 동 현 (Donghyeon Cheon)
1995년 2월 : 고려대학교 수학과 이학사
1997년 8월 : 고려대학교 대학원 수학과 이학석사
2001년 2월 : 고려대학교 대학원 수학과 이학박사
1999년 9월~2001년 8월 : 고려대학교 기초과학연구소 연구원
2001년 9월~현재 : 한국정보보호진흥원 암호기술팀 선임연구원
관심분야 : 암호학, 정보보호

전 길 수 (Kilsoo Chun)
1991년 2월 : 서강대학교 수학과 이학사
1993년 2월 : 서강대학교 대학원 수학과 이학석사
1998년 2월 : 서강대학교 대학원 수학과 이학박사
1998년 10월~1999년 9월 : 서강대학교 기초과학연구소 박사후 연구원
2001년 3월~2001년 6월 : 서강대학교 컴퓨터학과 연구교수
2001년 7월~현재 : 한국정보보호진흥원 암호기술팀 선임연구원
관심분야 : 암호학, 정보보호

강 성 우 (Sungwoo Kang)
1996년 2월 : 중앙대학교 수학과 이학사
2001년 8월 : 서울대학교 대학원 수학과 이학석사
2000년 12월~현재 : 한국정보보호진흥원 암호기술팀 연구원
관심분야 : 암호학, 정보보호

현 진 수 (Jinsu Hyun)
2000년 2월 : 한양대학교 수학과 이학사
2002년 2월 : 한양대학교 대학원 수학과 이학석사
2002년 1월~현재 : 한국정보보호진흥원 암호기술팀 연구원
관심분야 : 암호학, 정보보호

김 승 주 (Seungjoo Kim)
본호의 "고속 암호연산 프로세서 개발현황" 저자 소개 참조.

장 청 룡 (Chung-ryong Jang) 종신회원
1980년 2월 : 성균관대학교 전자공학과 졸업
1986년 8월 : 연세대학교 대학원 전자공학과 석사

1994년 2월 : 성균관대학교 대학원 정보공학과 박사
1979년 12월 ~ 1983년 12월 : 한국전자통신기술연구소(현, ETRI) 연구원
1984년 1월 ~ 1997년 1월 : 한국통신 연구개발본부 선임연구원
1997년 3월 ~ 현재: 경동대학교 정보보통신공학부 부교수
관심분야 : 보안제품 시험, 통신망 보호, 블록암호