情 報 保 護 學 會 誌
第 11 券 第 6 號, 2001. 12

블록암호 표준화 동향

장 청 룡*, 차 재 현**, 주 학 수***, 윤 선 희***, 김 승 주***

요 약

지식정보사회에서 모든 유통 및 관리 정보의 보호를 위하여 다양한 형태의 보호서비스가 활용되고 있다. 이러한 보호 서비스 중에서 민감한 정보의 비밀성을 보장하기 위한 암호 기법의 연구 개발과 이를 전자정부의 구현과 전자상거래와 같은 사업에의 적용에 따른 시장 점유와 연계된 표준화 활동이 암호기술 선진국을 중심으로 전개되고 있다. 이에 대하여 우리나라에서도 한국정보보호진흥원을 중심으로 국내 정보보호 분야 전문가들과 함께 개발하여 이미 TTAS.KO-12.0004(1999. 9)로 단체 표준화한 SEED를 지난 ISO/IEC JTC 1/SC 27 동경회의(2000. 10)에 제안하여 최근 국내에서 산업자원부 기술표준원이 개최한 ISO/IEC JTC 1/SC 27 서울회의(2001. 10)를 통하여 3차 WD에 수용되기에 이르렀다. 본 고에서는 비밀성 서비스를 지원하는 블록 암호 알고리즘의 지역(AES, NESSIE, CRYPTREC) 및 국제(ISO/IEC JTC 1) 표준화활동을 분석 정리하고 특히 ISO/IEC JTC 1/SC 27에서 블록 암호 회의를 통한 SEED의 국제표준화 활동을 소개하기로 한다.

Ⅰ. 서 론

지식정보사회의 성숙에 따라 정보의 재화가치로의 인식으로 이의 보호에 대한 의식은 점차 제고되고 있으며 이에 대한 정책의 수립과 구체적인 실천이 국가기관은 물론 산업체와 개인에 이르기까지 다양한 형태로 전개되고 있다. 최근 지식기반사회에서 인터넷의 이용증가에 힘입어 선진국은 물론 국내에서도 대 국민 행정 서비스의 개선 및 효율화를 위한 전자정부의 구현과 전자상거래의 활성화가 촉진되고 있으며 이에 역기능 작용을 하는 다양한 형태의 컴퓨터 범죄에 대한 대응 방안으로 법·제도적 조치와 기술적 조치가 취해지고 있다[1, 2, 3, 4].

이러한 기술적 대응 조치의 하나로 암호기술을 이용하는 것이 일반적인 추세이다. 더욱이, 대 국민 정보를 활용하는 전자정부의 구현에 있어 국민의 사생활 정보와 다양하고 민감한 정보의 보호 문제 해결은 반드시 선행되어야 하며 또한 전자상거래 처리 과정에서 유통되는 고객들의 사생활 정보, 거래 정보, 기업 정보 등의 적절한 보호 조치는 필수적이 되고 있다.

특히, 통신망에 유통되는 정보의 비밀성을 유지하기 위한 수단으로는 블록 암호의 DES와 공개키 암호의 RSA의 사용이 보편화되어 왔으며 이러한 알고리즘은 산업계의 사실상의 표준으로 자리잡고 있으며 미국의 연방 표준(FIPS), IETF 표준 나아가 ISO 표준으로 채택되어 왔다.

본 고에서는 비밀성의 보장을 위하여 이의 처리 속도에 있어 효율적이고 안전한 블록암호에 대한 표준화 활동을 중심으로 소개하며, 이를 위하여 먼저 미국을 중심으로 하는 AES Project, 유럽연합을 중심으로 하는 NESSIE Project, 일본을 중심으로 하는 CRYPTREC Project, 그리고 이들의 표준화를 세계적으로 통합하는 ISO/IEC JTC 1 Project에 대하여 이들의 주요 표준화 활동을 정리하기로 한다. 또한, 1999년 이 후 암호 알고리즘에 대한 운영 정책을 등록제에서 표준화로 바꾼 ISO/IEC JTC 1/SC 27의 활동 중 특히, 국내 개발 블록암호 알고리즘인 SEED의 국제 표준화를 위한 활동에 대하여 소개하기로 한다.

* 경동대학교 정보통신공학부 (crjang@kl.ac.kr)
** 산업자원부 기술표준원 (chajh@ats.go.kr)
*** 한국정보보호진흥원(KISA) ({hsju, shyoon, sjkim}@kisa.or.kr)

Ⅱ. 블록암호 국제 표준화 동향

블록암호 알고리즘에 있어 DES의 경우 1993년 평가에서 보안상의 취약성 때문에 이용상의 문제점을 인식하여 미국을 비롯한 유럽, 일본의 암호기술 선진국들에서는 이의 개선에 대한 연구를 꾸준히 해오고 있다[11, 14, 16].

한편, 국내에서도 한국정보보호센터가 주관이 되어 국내 전문가들과 공동으로 블록 암호알고리즘인 SEED를 개발하여 1999년 9월 TTAS.KO-12.0004로 단체 표준화를 하였다[1, 3, 4, 6].

이와 같이 민감한 정보의 비밀성을 보장하기 위한 암호 기법의 연구 개발과 이를 전자정부의 구현과 전자상거래와 같은 사업에의 적용에 따른 시장 점유와 연계된 표준화 활동이 암호기술 선진국을 중심으로 지역적인 표준화를 초월하여 국제적인 표준화장으로의 움직임이 ISO/IEC JTC 1/SC 27 콜럼비아 회의('99. 10)에서 제안되었다. 최근 이의 표준화를 위한 후보 알고리즘의 제안을 회원국들에 요청하여 이를 모집하고 이를 바탕으로 표준안을 작성하고 있다. 우리나라에서도 국내 정보보호 분야 전문가로 구성된 암호알고리즘 TFT가 한국정보보호센터의 협력 하에 SEED를 동경회의(2000. 10)에 제안하여 이의 표준화 활동에 적극 참여하고 있다[3, 7, 8, 9, 10].

1. AES Project

민감한 정보의 비밀성을 유지하기 위한 수단으로는 이용해 온 DES는 보안상의 결함으로 차세대 암호알고리즘으로 대체하려는 활동이 미국의 국립표준국(NIST)에서 주관이 되어 전자상거래 등의 업무에 활용할 수 있는 암호 알고리즘 표준화를 위한 AES(Advanced Encryption Standard) 프로젝트가 완료되었다. 최근 제 2 라운드(1999년 8월 ~ 2000년 5월) 수행의 결과로 5개의 최종 후보알고리즘(MARS(IBM), RC6(RSA), TWOFISH (Schneier외 5인, 미국), Rijndael (Daemen, Rijmen, 벨기에), SERPENT (Anderson, Biham, Knudsen ; 영국, 이스라엘, 덴마크))이 선정·발표되었다. 이러한 후보알고리즘 평가에 있어 NIST는 1차 평가에서는 구현상의 문제점을 검증하였고 2차 평가에서는 암호학적 분석보다는 각 알고리즘이 수학적으로 최적 구현되었는지에 대한 효율성 평가에 중점을 두고 있다고 밝혔다. AES 후보알고리즘의 암호학적 분석은 공개적 과정을 거쳐 수행되었으며 2000년 10월 AES 최종 알고리즘으로 Rijndael이 선정, 발표되기에 이르렀고 현재 이를 FIPS로 표준화하는 과정에 있다[3, 4, 11, 12, 13].

이와 같이 AES가 결정될 때까지의 과정은 공개적인 과정이었다고 할 수 있다. DES의 선정 때와 같이 불투명한 과정은 아니다. 약 3년 가까이 전 세계의 암호학자가 철저하게 조사한 결과 충분히 안전하고 처리 효율도 좋다고 증명된 AES(Rijndael)는 FIPS라는 규격의 틀을 넘어서 사실상의(de facto) 표준 암호알고리즘으로서 이용될 것이다. 또한 기술적인 면보다 미국의 차세대 표준화 암호 알고리즘이 유럽에서 나왔다는 사실이 단점이 되는데 심리적으로 플러스 요인으로서 작용하였다고도 생각된다. 향후 Rijndael의 이용 확대는 기본적으로 AES로서 FIPS화된 후 ANSI화, ISO화는 물론 IETF RFC화의 과정을 거치게 될 것이다[4, 11, 13].

2. NESSIE Project

유럽에서는 제 5차 R&D 프로젝트 프레임워크(1998~2002)의 일환으로 전자서명, 무결성 및 암호화에 적합한 새로운 암호기법을 개발하고 그 결과 기법들을 표준화하기 위하여 IST 프로그램으로 성립된 NESSIE(New European Schemes for Signature, Integrity, and Encryption) 프로젝트(IST-1999-12424, 2000 ~ 2002)를 추진하고 있다. 이 프로젝트의 목표는 선정된 암호 프리머티브를 널리 보급시킴과 동시에 공개 토론의 장을 통하여 그 선정 결과에 기초한 합의를 얻는 것에 있다. 그리고 최종적으로는 유럽 연합으로부터의 강한 지위를 확보함과 동시에 유럽 암호산업의 강화를 목표로 한다[4, 14].

이는 2000년 1월부터 2001년 6월까지를 1단계 그리고 2001년 7월부터 2002년 12월까지를 2단계로 하여 이스라엘과 노르웨이를 포함한 4개 EU회원국의 총 7개 기관이 참여(당초 이태리(Fondazione Ugo Bordoni)를 포함하여 8개 기관이었으나 2차년도에 사퇴함)하고 있다. 1단계에서는 암호 프리머티브들을 공개 모집하여 이를 평가하고 2단계에서는 적합한 것들을 선정하여 표준화 계획을 잡아 최종 선정하는 것으로 하고 있다.

2000년 3월에 개시하여 2000년 9월에 마감한

- Block ciphers
  - 64-bit block ciphers
    - CS-Cipher
    - Hierocrypt-L1
    - IDEA *
    - Khazad *
    - MISTY1 *
    - Nimbus
  - 128-bit block ciphers
    - Anubis
    - Camellia *
    - Grand Cru
    - Hierocrypt-3
    - Noekeon
    - Q
    - SC2000
  - 160-bit block ciphers
    - SHACAL *
  - variable length block ciphers
    - NUSH: 64, 128, and 256-bit
    - RC6 : at least 128-bit *
    - SAFER++: 64 and 128-bit *
- Synchronous stream ciphers
  - BMGL *
  - Leviathan
  - LILI-128
  - SNOW *
  - SOBER-t16 *
  - SOBER-t32 *
- Message authentication codes
  - Two-Track-MAC *
  - UMAC *
- Collision-Resistant and one-way hash functions
  - Whirlpool *
- Asymmetric encryption schemes
  - ACE Encrypt *
  - ECIES *
  - EPOC *
  - PSEC *
  - RSA-OAEP *
- Asymmetric digital signature schemes
  - ACE Sign
  - ECDSA *
  - ESIGN *
  - FLASH
  - QUARTZ *
  - RSA-PSS *
  - SFLASH *
- Asymmetric identification schemes
  - GPS *

주 : *는 제 2 단계 평가 경합 암호 프리머티브.

〔그림 2-1〕 NESSIE 평가 대상 암호 프리머티브

공모에서는 16개의 블록 암호(Hierocrypt-3 /-L1, Khazad, MISTY1, RC6, SAFER++, SC2000 등), 5개의 스트림 암호, 4개의 해쉬함수와 MAC, 5개의 비대칭 암호 기법, 7개의 전자서명 기법, 1개의 비대칭 식별기법들이 제안되었다. 이에 대한 발표는 당초 계획보다 1개월 지연되어 2000년 11월에 제 1차 NESSIE workshop을 통하여 발표되었으며 이들 제안에 대한 기본 평가 결과는 2001년 6월에 발표되었다. 이를 기초로 제 2 단계 평가를 추진하고 있으며 그 진행 결과를 2001년 9월 제 2차 NESSIE workshop에서 정리되었으며 최근 과제 책임자인 Bart Preneel(벨기에 Katholieke Universiteit Leuven)에 의해 발표된 제 2단계 경합을 위한 암호 프리머티브들은 (그림 2-1)과 같다[4, 14, 15]. 여기서, 블록 암호와 관련하여 64-비트 후보로는 IDEA, Khazad, MISTY1, 128-비트 후보로는 Camellia, 160-비트 후보로는 SHACAL, 그리고 가변 길이 후보로는 RC6과 SAFER++가 선정되었다.

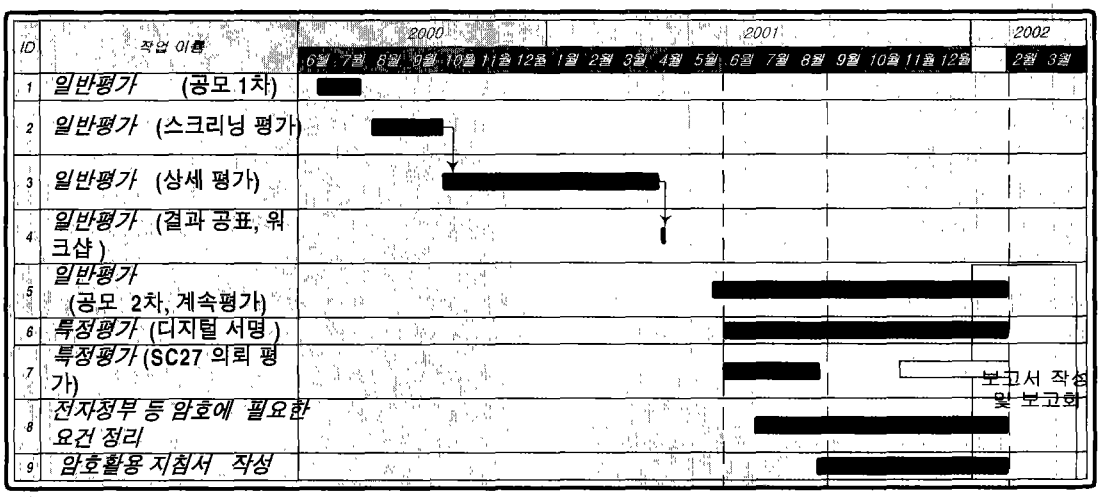
3. CRYPTREC Project

일본에서는 2003년 전자정부의 구현을 목표로 이에 요구되는 공통적인 보안 기반 기술을 확보하기 위한 과제를 추진하고 있다. 이 과제는 경제산업성(구, 통산성)으로부터 위탁을 받은 정보처리진흥사업협회(IPA : Information Promotion Association)의 보안센터(ISEC : Information SEcurity Center)와 통신방송기구(TAO : Telecommunication Advancement Organization)가 주관이 되어 활동하고 있다[4, 16, 20].

본 사업은 암호기술 프리머티브들에 관한 공모, 평가 및 표준화에 이르기까지 일련의 작업으로 이루어지며 일본 최고 수준의 전문가들로 구성된 암호기술평가위원회(CRYPTREC : CRYPTography Research and Evaluation Committee)에 의해 평가가 이루어진다. 평가의 시간 계획은 2000년 6월 13일부터 1차 일반 공모를 개시하여 2000년 7월 14일까지 이를 마감하고 2000년 10월초에 상세평가의 준비로서 일차 스크리닝 결과를 발표하였다. 본 사업과 관련한 비밀성을 위한 프리머티브인 블록암호 기법으로는 13개가 제안되었으나 스크리닝 결과 10개만 상세평가를 하기로 하였으며 이의 세부기법은 다음의 〔표 2-1〕과 같다[4, 16, 17]:

〔표 2-1〕 CRYPTREC 블록 암호 부문 제 1차 평가 후보

◦ 64-비트(4개)	◦ 128-비트(6개)
- CIPHERUNICORN-E	- CIPHERUNICORN-A
- FEAL-NX	- Camellia
- MISTY1	- RC6
- Hierocrypt-L1	- SC2000
	- MARS
	- Hierocrypt-3



〔그림 2-2〕 CRYPTREC의 암호 프리머티브 평가 일정

이에 추가 평가로 시행하는 암호기법 중 블록 암호기법으로는 현재 FIPS 46-3인 Triple DES와 AES로 최종 표준화 중인 Rijndael이 있다. 한편, 2000년도 암호기술에 관한 평가 보고를 위하여 CRYPTREC workshop이 2001년 4월 18일 개최되었으며 여기서는 세계 암호 표준화 활동에 대한 소개와 CRYPTREC의 암호기술 평가보고 및 향후 계획이 발표되었다. 더욱이, 당초 ISO/IEC JTC 1/SC 27 동경회의에서 차기 회의인 오슬로 회의에 CRYPTREC의 평가 결과로 선정된 알고리즘들을 제안하기로 하였으나 이의 선정을 위하여 좀더 시간이 필요한 것으로 정리되었다[4, 16, 17].

특히, 블록 암호에 대하여는 다음과 같은 1차 평가결과를 얻었다. 한편, 여기서 처리속도는 Triple DES(Pentium III 급 전산환경에서 측정)와의 상대 비교이다[17].

〈 64-비트 블록 암호 부문〉

- CIPHERUNICORN-E

어떤 취약점도 발견 안됨, 복잡한 구조적 특성으로 이의 안전성을 정확히 평가가 곤란함. 따라서 지속적인 평가가 요구되며 이의 처리 속도는 "느린 그룹"으로 분류됨.

- FEAL-NX

FEAL-32X는 이론상 299 시간 복잡도로 해독될 수 있어 장기적인 생명주기를 갖는 것으로는 이의 사용이 권고될 수 없음.

- MISTY1

어떤 취약점도 발견 안됨, 이의 처리 속도는 "고속 그룹"으로 분류됨.

- Hierocrypt-L1

어떤 취약점도 발견 안됨, 이의 처리 속도는 "고속 그룹"으로 분류됨.

- Triple DES

FIPS나 혹은 여타 표준으로 제정된다면 안전성 측면에서는 문제가 없음.

〈 128-비트 블록 암호 부문〉

- CIPHERUNICORN-A

어떤 취약점도 발견 안됨, 복잡한 라운드 함수의 특성으로 이의 안전성을 정확히 평가가 곤란함. 따라서 지속적인 평가가 요구되며 이의 처리 속도는 "느린 그룹"으로 분류됨.

- Camellia

어떤 취약점도 발견 안됨, 이의 처리 속도는 "고속 그룹"으로 분류됨.

- RC6

어떤 취약점도 발견 안됨, 이의 처리 속도는 Pentium III에서 가장 빠르지만 소프트웨어로의 처리는 구현 플랫폼에 대단히 종속적임.

- SC2000

어떤 취약점도 발견 안됨, 이의 처리 속도는 "고속 그룹"으로 분류됨.

- MARS

어떤 취약점도 발견 안됨, 이의 처리 속도는 IBM에서 이의 제품화를 위한 어떤 의지도 없어 평가하지 못함.

- Hierocrypt-3

어떤 취약점도 발견 안됨, 이의 처리 속도는 "고속 그룹"으로 분류됨.

- Rijndael

AES 암호로 선정되어 신뢰할 만하다고 간주됨. 전자정부에의 적용을 위하여 FIPS 버전에 대한 재평가가 권고됨.

이에 추가로 CRYPTREC에서는 2001년 8월 1일~2001년 9월 27일까지 2차 일반 공모 및 전자서명과 SC27 의뢰의 특정 평가를 추진하고 있으며 이는 (그림 2-2)에 보여 지고 있다. 이 과정을 통하여 2000년에 이어 계속해서 공모하고, 응모된 암호기술에 관하여 전문적 식견 및 객관적인 입장에서 평가·조사를 실시하며 전자 정부의 시스템 구축에 있어 이용 가능한 기술에 대해 안전성, 구현성 등의 특징을 리스트-업 한다[4, 18].

이 결과는 전자 정부에 있어 암호 기술을 이용할 때의 참고로서 정부 내에서 다양한 형태로 이용된 것이 예상된다. 2000년 사업 목표와 금년도 사업 목표 상의 큰 차이는 없으나 용어의 사용이 e-정부에서 e-Japan으로 변하면서 세계화를 지향하고 있음을 읽을 수 있다[18].

4. ISO/IEC JTC 1 Project

ISO/IEC JTC 1에서는 비밀성을 보장하기 위한 암호알고리즘에 대하여 1999년 상반기까지는 특정 알고리즘을 표준화하여 정하기보다는 등록제로 하여 암호 알고리즘의 등록 절차를 표준화(ISO/IEC 9979, 1991(제정), 1999(개정))를 하여 운용하고 있으며 회원국들로부터의 암호 알고리즘 등록 엔트리는 '99년 7월 현재 20개에 이르고 있다[21].

그러나, 새로운 밀레니엄에 요구되는 암호 알고리즘으로 미국에서 추진하는 AES 및 유럽 연합에서 추진하는 NESSIE의 영향으로 1999년 ISO/IEC JTC 1/SC 27 전체회의(미국 콜럼비아, '99. 10)에서 암호 알고리즘 표준화를 위한 신규 과제화 제안을 하기에 이르렀다. 이러한 제안에 따라 각 회원국들로부터 후보 알고리즘에 대한 제안을 받아 2000년 봄 런던회의(2000. 4)에서 논의하였으나 제안 지침의 모호성 및 제출 기간의 촉박 등의 문제를 인식하여 수정된 제안 지침(ISO/IEC JTC 1/SC 27 N2563, Call for contributions on NP 18033: Encryption algorithms)에 의거 2000년 9월 15일까지 각 회원국들로부터 공개키, 블록, 스트림 기법에 대한 후보 암호 알고리즘의 제안을 받아 그 해 가을 동경회의(2000. 10)에서 공개키 7개, 블록 15개, 스트림 1개가 제안되었다. 오슬로회의(2001. 4)에서 한국의 Zodiac과 미국의 Serpent와 Twofish가 철회되어 블록 암호는 11개의 후보로 [표 2-2]와 같이 정리되었다[7, 8, 9, 10, 22, 23, 24].

여기서, Zodiac은 이론적 공격이 가능한 것으로 지적되었으며 Serpent 와 Twofish는 미국에서 지난 ISO/IEC JTC 1/SC 27 동경회의에의 제안시 AES가 단일로 선정되지 않은 상태여서 5개 후보를 모두 제안하였으나 2000년 10월 AES로 Rijndael이 최종 선정됨에 따라 이를 단일화하여 나머지 알고리즘을 철회하였다. 한편, 이들중 2개의 알고리즘은 스웨덴(RC6) 및 일본(MARS)과 공동 제안한 것으로 제안 회원국의 입장을 고려하여 이를 그대로 유지하기로 하였다.

금년 서울회의(2001. 10)에서 일본은 CRYPTREC의 평가 결과로 64비트로 MISTY1을 제안하고 128비트로 Camellia를 제안하였다. 아울러, 한국에서 제안한 Xenon에 대한 이론적 공격가능성을 제시하였다. 한편 NESSIE에서는 특정 선정 결과를 발표하기보다는 자체 제 2단계 경합 암호 프리머티브를 통보하고 과제의 종료 시까지 지속적으로 평가하여 그 결과를 제시하기로 하였다[15, 25].

[표 2-2] ISO/IEC JTC 1/SC 27 서울회의 결과 후보 암호 알고리즘

제안국	구분	알고리즘 명	제안국	구분	알고리즘 명
캐나다	블록	CAST-128	일본	블록	MARS**
독일	공개키	ACE			CIPHERUNICORN**
대한민국	블록	SEED			MISTY1
		XENON**			Hierocrypto**
		ZODIAC*			Camellia
스웨덴	블록	RC6			
미국	블록	AES		공개키	EPOC
	공개키	ECIES			PSEC
		RSA-OAEP			HIME
스위스	블록	IDEA		스트림	MULTI-S01

주 *: 오슬로 회의(2001. 4) 철회 블록 암호 후보
**: 서울 회의(2001. 10) 철회 블록 암호 후보

따라서, 서울회의 결과 WD18033-1, Annex A

의 A.1 Selection criteria의 각 기준에 맞는 제안 후보로는 현재의 WD에 수용된 TDEA와 AES 이외에 CAST-128, IDEA, MISTY1, Camellia, SEED (및 RC6)이 포함될 수 있음을 결의하고 3차 WD의 작성을 위하여 해당 회원국들로부터 제안 후보에 대한 표준문서를 금년 말까지 제출하도록 하였다. 서울 회의 결과 후보 암호 알고리즘들은 다음의 [표 2-2]와 같이 정리되었다[26, 27].

Ⅲ. ISO/IEC JTC 1/SC 27의 블록암호 표준화 회의 주요 논의 사항

1. ISO/IEC JTC 1/SC 27/WG 2 제 20차 런던 회의[7, 8, 9]

1.1 회의 개요

가. 일시 및 장소

- 일시 : 2000년 4월 4일 13:00 ~ 17:00
- 장소 : 영국 런던 BSI 411 회의실

나. 검토 문서

- SC27 N2521(암호알고리즘 표준화 신규과제 (New Work Item)의 투표 요약)
- SC27 N2530(한국 등 6개 회원국 제안)
- SC27 N2535 (Swiss contribution)
- SC27 N2568 (Belgium contribution)

1.2 주요 토의 내용

암호알고리즘 표준화 신규 과제화의 승인여부에 대한 SC 27 N2488(이후 "SC 27" 생략) 문서의 투표결과가 정리된 N2521을 검토하였다. 과제 자체에 대한 반대는 네덜란드와 미국뿐이었다. 네덜란드는 AES의 선정결과가 제출되기에 너무 일정이 시급하며 AES가 제출되지 않는 상황에서는 이의 표준화는 의미가 없다는 것이었다. 미국의 반대 이유도 우선은 제안 일정이 촉박하다는 것이었고, 너무 포괄적인 조건으로 Call for Contribution (N2477)을 하였다는 이유로 반대하였다. 그러나 미국도 다른 항목들은 다 찬성하였고, 우선 5개의 AES 후보를 모두 제안하되 나중에 결정되는 것만을 표준으로 선정하기로 하고, AES가 포함될 세부과제에 editor를 맡기로 하였다.

제안 암호 알고리즘으로는 Block cipher가 15개, 그리고 Asymmetric cipher는 3개가 제안되었다. 이외에도 미국은 ECIES(Elliptic Curve Integrated Encryption Scheme)와RSA-OAEP (Optimal Asymmetric Encryption Padding)라는 두 개의 Asymmetric cipher를 차기 회의에 제안하기로 하였다. 또한 Tripple DES가 TC68에서 표준이 되고 있으므로 포함되어야 한다는 의견도 있었고, 다른 알고리즘이나 기 제출된 알고리즘의 수정 또한 허용되어야 함에 의견이 모아졌다.

표준은 Multi-part의 표준으로 하기로 하고 표준문서번호 18033에 전체 제목을 Encipherment Algorithm, Part 1: General, Part 2: Asymmetric Ciphers, Part 3: Block Ciphers, Part 4: Stream Ciphers로 하기로 하였고 각 Part의 Acting Editor를 Chris Mitchell(영국), Victor Shoup(독일), Foti(미국), Sakurai(일본)가 각각 맡기로 하였다.

가장 논란이 많았던 부분은 선정 절차 및 기준이었다. 우선 SC27이 Evaluation을 떠맡을 수는 없지 않느냐는 것이 대세이었으며 모두가 선정은 필요하며 그 절차와 기준에 신중을 기하자는 의견이었다. 그리고 단일 표준이 아니고 무언가 다른 것이 갖지 않는 표준이 있다면 여러 개의 표준이 각 Part별로 결정될 수 있다는 것이 중론이었다.

Evaluation에 관한 다른 의견들은 AES를 통과한 것이라면 충분하다는 것과, 제안국 이외의 다른 국가 혹은 국제표준기관, research community 등 믿을 만한 제 3자들이 평가한 것이면 받아들일 수 있지 않겠는가 하는 의견도 있었다. 또한 security proof가 가능하면 다른 평가가 필요하지 않을 수도 있다는 의견도 있었다.

선정기준은 확정된 것이 아니고 Chris Mitchell이 5월 10일까지 초안을 만들어서 각 회원국에 회람시켜 그들의 의견을 수렴하여, 그 결과를 8월 CRYPTO 학회기간에 관련회의를 거쳐 선정기준을 확정하기로 하였다.

그러나, 최소한 AES는 Fast Track(CD, DIS 등의 투표절차에 필요한 시간을 훨씬 줄여서 빨리 진행시키는 것)으로 처리하자는 의견도 있었다.

그밖에 관련 사항들로는 일본이 2000년 4월부터 전자정부의 구현을 위하여 이용할 모든 종류의 암호 알고리즘의 표준을 정하기 위한 절차가 행하여지는데 ISO의 암호 알고리즘 선정 criteria가 정해지면 그것을 참고하겠다고 하였고, 암호알고리즘 수출규제 문제가 없으며 공개되어 있는 경우에만 일본 이

외의 국가로부터의 제안이 가능하다고 하였다.

2. ISO/IEC JTC 1/SC 27/WG 2 제 21차 동경 회의[3, 10, 11, 14, 16, 22]

2.1 회의 개요

가. 일시 및 장소 :

- 2000. 10. 18(수) 13 : 00 ~ 17 : 30,
  10. 19(목) 09 : 15 ~ 10 : 30,
- 동경 미나토구 시바코엔 기계진흥회관 6층 61호 회의실

나. 검토 문서 :

- SC27 N2656r1 : National Body contributions on NP 18033 " Encryption Algorithms" in response to document SC N2563
- SC27 N2723 : New Text of 1st WD 18033-1

2.2 주요 토의 내용

가. 제 1부 : Genéral

Editor인 영국의 Chris Mitchell이 준비한 작업문서 초안(문서번호 부여받지 못함)에 대하여 별다른 이견은 없었으며 각 부의 기본 모델을 수용하여 작성하기로 하였다.

나. 제 2부 : Asymmetric Cipher (비대칭 암호 알고리즘)

Editor인 독일의 V. Shoup이 준비한 제안 알고리즘의 기본적 안전성의 이론 근거(RO(random oracle), CDH(computational Diffie-Hellman), ElGamal, DDH(decisional D-H), Elliptic Curve, 소인수분해 등)에 의한 분류에 의한 모델링을 하고 제안 알고리즘들 중 유사한 것은 그룹별로 통일시켜 정리하기로 하였다.

- 우선 (1) RSA-OAEP와 (2) EC-El Gamal의 변형인 ACE 및 PSEC(가능하면 ECIES도)를 통합한 하나의 일반형을 다음 WD에 포함시키고 다른 것들은 차차 고려하기로 하고,
- 제안 알고리즘의 선정은 제3의 객관화될 수 있는 기관 또는 전문가들에 평가(NESSIE, CRYPTREC 등)한 결과를 우선적으로 고려하기로 하며 이를 위하여 특장점(키 설정), 메시지 길이(고정, 임의), 적용 분야, 실용성, 효율성, 보급 등을 검토하기로 하였다.

다. 제 3부 : Block Cipher (대칭 암호알고리즘)

제안 알고리즘의 선정은 제 3의 객관화될 수 있는 기관(AES, NESSIE, CRYPTREC 등) 또는 전문가들에 평가 결과를 우선적으로 고려하기로 하고 평가 기관들의 결과를 다음과 같이 수용하기로 하였다.

- AES : Rijndael
- CRYPTREC : 응모(기간(2000. 6. 13~2000. 7. 14)를 마감하고 2001. 3까지 평가 완료 예정(평가 대상은 현재 일본이 SC27에 제안된 후보를 포함하여 RC6, Rijndael 등이 추가로 평가될 예정)
- NESSIE : 응모(2000. 9 마감) 및 평가 중 작성 예정인 WD에는 Rijndael과 TDEA 만을 넣어서 만들고 다른 알고리즘들의 포함은 추후 고려하기로 하였다.

라. 제 4부 : Stream Cipher (스트림 암호 알고리즘)

제안국인 일본의 발표 후 토의하였으며 editor가 최근 IMT 2000에서 암호알고리즘 표준으로 선정된 Kasumi를 키 스트림 생성기로 이용하는 방안에 대하여 이와 유사한 것을 본 표준에서 수용할 것의 여부를 제안하여 본 표준의 해당 절에서 다음과 같이 규정에 대하여 논의하고 이러한 방식으로 접근하기로 하였다.

- PRSG(Pseudo random sequence generation)
- Using block cipher에서 ISO/IEC 10116 이용(스트림 사이퍼의 키 스트림 생성에 적용을 규정)
- Dedicated sequence generator(예, PANAMA, SEAL 등)
- Usage of PRSG

3. ISO/IEC JTC 1/SC 27/WG 2 제 22차 오슬로 회의[4, 5, 23, 24]

3.1 개 요

가. 일시 및 장소

- 회의명 : SC 27/WG 2 회의 중 암호알고리즘 회의
- 일시 : 2001년 4월 24일(화) ~ 4월 26(목)
- 장소 : 노르웨이 오슬로 House of Industry

대회의실

나. 검토 문서

- ISO/IEC WD 18033-1(Part 1. General)
  - SC 27 N2723 : Text of 1st ISO/IEC WD 18033-1 Part 1: General
  - SC 27 N2806 : Summary of NB Comments
  - SC 27 N2848 : Japanese NB contribution on NP 18033-1 and 18033-3
- ISO/IEC WD 18033-3(Part 3. Block Cipher)
  - SC 27 N2725 : 18033-3의 작업문서(WD)
  - SC 27 N2742 : 동경회의 보고
  - SC 27 N2814 : Zodiac 해독
  - SC 27 N2820 : 관련 64-비트 블록 사이퍼의 포함에 대한 일본 제안 (SC 27 N2820r : 일본-한국의 기고로 현행화)
  - SC 27 N2848 : 알고리즘 선정을 위한 일본국 제안
  - SC 27 N2851 : 제안 알고리즘의 기술적 비교
  - SC 27 N2852 : MISTY와 KASUMI의 비교
  - SC 27 N2856 : CRYPTREC 보고
  - SC 27 N2859 : CRYPTREC 결과
  - SC 27/WG2 Oslo1 : Camellia의 발표
  - SC 27 N2925 : Hierocrypt의 암호학적 성질의 분석

3.2 주요 토의 내용

가. ISO/IEC WD 18033-1(Part 1. General)

SC 27 N2730(Report of the Tokyo meeting on NP 18033-1)에 준거하여 작성한 SC 27 N2723을 SC 27 N2806에서 제안된 각 회원국들의 의견을 논의하였으며 세부 토의 사항으로는,

- 본 표준의 목적 및 적용 범위를 비밀성(confidentiality)에 한정하는 암호 알고리즘의 표준화로 하고 무결성 및 인증에 관한 것은 별도의 표준화로 처리하는 것으로 함.
- 7절(본 표준(Part 1)에서의 알고리즘 선정기준)에 대하여 한국에서는 본 표준의 범위는 비밀성을 위한 알고리즘들을 표준화하는 것이지 암호 알고리즘의 선정에 대한 표현을 이 절에 수용함은 바람직하지 않음을 주장.
- 일본측에서 SC 27 N2848을 제시하면서 후보 암호알고리즘의 선정 절차를 Part 1의 7절을 보다 상세히 규정하는 것을 제안함.
- Editor인 Christ Mitchell의 중재로 7을 본 표준의 부기(Annex, Informative)로 처리하기로 하고 세부 내용은 다음과 같이 일본국의 일부 내용을 수용하기로 함:
  - 제 7절에서 7.1의 4인 maturity 절을 2가지로 나누어 처리하기로 함.
    + 사용의 광의성, 분석의 공개성, 고찰성
    + recognized organization으로부터의 endorsement.

나. ISO/IEC WD 18033-3(Part 3. Block Cipher)

먼저, 현 작업 문서(SC 27 N2725, TDEA와 AES만 포함)에 대한 토의로서,

- 미국은 AES에 대하여 2001년 5월 29일까지 의견수렴 기간에 있으며 최종 표준은 금년 10월에나 가능 함(본 연구보고서의 작성시까지 확인 안됨).
- TDEA의 안전성(예, 평문의 길이 등)을 부기(informative)로 포함시키기로 하고 이의 해당 내용을 미국 측에서 제공하기로 함.
- 부기에 DES를 추가하기로 함.
- TDEA 키 선택의 2가지 선택사항을 본문에 수용하고 그와 동치의 single-DES에 관한 선택사항은 삭제하기로 함(그러나 이를 주석으로 처리).

그 밖의 제안 알고리즘에 대한 논의로서는,

- 일본측의 기고문은 다음과 같은 내용으로 제안하였음:
  - 64-비트와 128-비트로 분류하여 MISTY1을 현재 수용된 Triple-DES에 추가로 수용시키자는 제안.
  - 그밖에 MISTY1과 KASUMI와의 차이, Camellia와 Hierocrypt에 대한 추가 기고문이 제안됨.
  - 오슬로회의까지는 일본으로부터 특정 후보가 제안되지 않았으며, 지난 동경회의에서 CRYPTREC의 평가결과를 보고하기로 되어 있었으나 아직 그 결과를 얻을 수 없어 금년 9월에 평가 결과가 나오므로 10월 서울 회의에 제안이 가능할 것임.
- NESSIE도 9월에 2차 평가 결과가 나오면

이를 제안할 것임.

3.3 토의 결과

한국 측은 Zodiac을 후보알고리즘에서 철회(SC 27 N2820r)하기로 하고, 미국에서는 Rijndael이 AES로 선정되어 이것만을 남기고 나머지는 철회하기로 하였다. 다만, AES finalist 후보로 제안된 것 중에서 다른 회원국으로부터 제안된 것(RC6, MARS)은 그대로 두기로 하였다.

일본국이 알고리즘 선정의 편의를 위하여 평가 기준에 의하여 비교표를 작성하여 금년 가을 서울회의에 제안하기로 하고 이에 SEED도 포함하여 처리하기 하였다. 그러나, 오슬로 회의보고(SC 27 N2919 : Oslo 회의보고)에는 이의 표현을 "현재의 알고리즘(TDEA, AES) 이외 알고리즘의 추가에 대한 고려에 앞서 더 많은 정보가 필요하므로 본 표준에 특정 알고리즘을 포함시키기 위한 이유에 대한 비교 정보를 제공하도록 모든 회원국(특히, 알고리즘 제안 NB)에게 요구하기로 함"으로 처리하였다.

최근, 일본의 2차 일반 평가에서 CRYPTREC 측에서는 오슬로 회의에서 자국대표가 SC 27 후보 알고리즘의 평가를 하겠다는 것에 대하여 구태여 한국의 SEED를 포함시켜 추진함이 자국의 이해에 별로 도움이 되지 않는다는 위원회의 입장으로 이 평가에 SEED를 포함시키려고 하지 않았다. 그러나 한국이 이를 원하는 경우 일반 공모를 하도록 권유하였다.

4. ISO/IEC JTC 1/SC 27/WG 2 제 23차 서울 회의[25, 26, 27]

4.1 개 요

가. 일시 및 장소

- 회의명 : SC 27/WG 2 회의 중 블록 암호알고리즘 회의
- 일시 : 2001년 10월 17일(수) 09:00 ~ 12:30
- 장소 : 서울 ASEM HALL 211호

나. 검토 문서

- SC 27 N2920 : 18033-3의 작업문서(2nd WD)
- SC 27 N2975rev1 : Summary of NB Comments from Japan, Korea, Sweden, Switzerland and UK
- SC 27 N2980 : Canadian NB contribution
- SC 27 N2989 : Japanese NB contribution (Camellia and MISTY1)

4.2 주요 토의 내용

가. 일본 (SC 27 N2975rev1 Attachment 1)

- 64비트 블록암호 : TDEA의 암복호화 처리 속도가 빠르지 않으며 H/W 구현시 크기가 작지 않음. 보다 좋은 다른 최소 하나의 알고리즘이 포함되기를 제안하며 이에 MISTY1을 제안함.
- 128비트 블록암호 : 복수 알고리즘의 수용을 제안하며 AES 수준에 버금 가는 안전성과 성능의 알고리즘으로 Camellia를 제안함.
  - Xenon의 공격가능에 대한 의견이 일본측 전문가들로부터 접수되었으며 금년 11월경 일본내의 학술발표회에서 발표 예정임.
  - 이번 서울회의까지의 최종 후보로는 다음의 알고리즘들이 고려될 수 있음;
    + 64-bit block cipher의 경우,
      · IDEA (Switzerland)
      · MISTY1 (Japan)
    + 128-bit block cipher의 경우,
      · Camellia (Japan)
      · RC6 (Sweden)
      · SEED (Korea)
      · CAST-128 (Canada)

나. 한국 (SC 27 N2975rev1 Attachment 2)

- Maturity에 대하여 SEED는 국내의 산업표준으로 자리 잡음(TTAS.KO-12.004, 1999). 또한 보급 현황으로 연구 기관 및 학계를 포함하여 330개 기관에 보급되었으며(2001년 6월말 현재) 한국은행의 주관으로 600개 이상의 가맹점에 의한 K-cash 시범사업이 작년 6월부터 진행됨.
- SEED의 성능에 대하여 H/W(8-비트 프로세서, complexity) 및 S/W 성능에 대하여 정리한 것을 설명함.

다. 캐나다 (SC 27 N2980)

- WD18033-1, Annex A의 A.1 Selection criteria의 각 기준에 맞추어 CAST-128의 제출이 문제가 없음을 선언함. 다음을 붙임으로 처리함.

- NIST의 AES 1st round status report
- The CAST-128 Encryption Algorithm (IETF Network Group RFC 2144, May 1997)

4.3 토의 결과

WD18033-1, Annex A의 A.1 Selection criteria의 각 기준에 맞는 제안 후보로는 현재의 WD에 수용된 TDEA와 AES이외에 CAST-128, IDEA, MISTY1, Camellia, SEED (및 RC6)이 포함될 수 있음.

4.4 향후 계획

- 2001. 12. 1 : 2차 WD의 서울회의 결과 정리 및 현행화
- 2001. 12. 31 : 3차 WD에 수용하기 위한 각 NB의 알고리즘 규격 본문 작성 및 제출 마감
- 2002. 1. 31 : 각 NB에 차기 베를린회의에 의견 제시 요청.

Ⅵ. 결 론

개인의 사생활 정보를 포함한 민감한 정보의 비밀성을 보장하기 위한 암호 기법의 연구 개발과 이를 전자정부의 구현 및 전자상거래와 같은 사업에의 적용에 따른 시장 점유와 연계된 표준화 활동이 암호 기술 선진국을 중심으로 전개되고 있다.

본 고에서는 비밀성 지원을 하는 암호 기법 중 블록암호를 중심으로 지역적인 표준화와 국제적인 표준화 동향을 정리하였다. 특히, 우리나라에서 산업 표준으로 자리잡은 128비트 블록 암호인 SEED를 국제 표준화를 주도하는 ISO/IEC JTC 1/SC 27에서의 국내 암호 알고리즘 TFT와 관계 전문가들의 적극적인 표준화 활동 참여를 회의별로 정리하였다. 특히, SEED를 동경회의(2000. 10)에 제안하여 최근의 서울회의(2001, 10)에 걸쳐 활동에 의한 현재 3차 WD에 수용되기에 이르기까지의 과정을 소개하였다.

앞으로 국내 관계 전문가들의 많은 관심과 참여를 통하여 우리나라의 개발 암호 기법인 SEED를 국제 표준화에 안정적으로 수용될 수 있도록 노력을 하여야 할 것이다. 더욱이, 암호 프리머티브의 체계적인 개발 보급을 위한 활동을 통하여 국내 암호 산업의 육성 및 발전에 기여될 수 있도록 관계 기관 및 전문가들의 관심의 요구된다.

참 고 문 헌

[1] 이홍섭 외, 정보보호기술개발 - 128비트 블록 암호알고리즘 (SEED) 개발 및 분석 보고서 (http://www.kisa.or.kr/technology/sub1/128-seed.pdf) , 한국정보보호센터, 1998. 12.

[2] 박성준, "국내 표준 블록 암호알고리즘(SEED) 활용방법", 제4회 정보보호 심포지움(SIS '99), 한국정보보호센터, pp. 575~599, 1999. 4.

[3] 장청룡 외, SEED의 ISO/IEC 국제표준화 추진(최종연구보고서, 암호기술 00-3), 한국정보보호센터, 2000. 12.

[4] 장청룡, "암호알고리즘 국제표준화 동향", 제7회 정보보안기술 표준화 워크샵(SWIST-2001), pp. 327 ~ 336, 2001. 8.

[5] 이필중, 장청룡, 강경희, 임영숙, "ISO/IEC JTC 1/SC 27(정보보안기술) WG2 22차 오슬로 회의 참가 보고", 정보보호학회지, 제11권 제3호, pp. 65~74.

[6] 정보통신단체표준(TTAS.KO-12.0004), http://www.kisa.or.kr/evaluation/webdriver?MIval=hh_3_ tta.

[7] ISO/IEC JTC 1/SC 27, "A Call for Contributions to a New Work Item Proposal on "Encryption Algorithms"", ISO/IEC JTC 1/SC 27 N2477, 1999. 12.

[8] ISO/IEC JTC 1/SC 27, "Summary of Voting on JTC 1 N6009(SC 27 N2488, Proposal for a New Work Item on Encryption Algorithms)", ISO/IEC JTC 1/SC 27 N2521, 2000. 3.

[9] ISO/IEC JTC 1/SC 27, "National Body Contributions on NP 18033 "Encryption Algorithms" in Response to SC 27 N2477", ISO/IEC JTC 1/SC 27 N2530, 2000. 3.

[10] ISO/IEC JTC 1/SC 27, "National Body Contributions on NP 18033 "Encryption Algorithms" in Response to SC 27 N2563

(ATT. 3 Korean Contribution)", ISO/IEC JTC 1/SC 27 N2656r1(n2656_3.zip), 2000. 10.
[11] AES project description, http://csrc.nist.gov/ encryption/aes/aes_home.htm.
[12] The proposed selection of Rijndael as the AES, http://www.nist.gov/public_affairs/ releases/ g00-176.htm#release
[13] NIST, "NIST Seeks Final Comments on AES", NIST Update, http://www.nist.gov/ public_affairs/update/upd010305.htm# computer, 2001. 5.
[14] NESSIE project description, http://www.cosic.esat.kuleuven.ac.be/ nessie/.
[15] Bart Preneel, "NESSIE Project Announces Selection of Crypto Algorithms", September 24, 2001.
[16] CRYPTREC home page, http://www.ipa.go.jp/security/enc/CRYPTREC/index.html.
[17] 暗號技術評價報告書 「CRYPTREC REPORT 2000」, 情報處理振興事業協會, 平成13年 3月, http://www.ipa.go.jp/security/fy12/report/cryptrec-report2k.pdf
[18] CRYPTREC, "平成13年度暗號技術の公募(8/1~9/27)について", http://www.ipa.go.jp/security/enc/CRYPTREC/fy13/cryptrec 20010731_ call.html.
[19] 情報處理振興事業協會, 通信放送機構, "平成13年度 暗號技術公募要領", 平成13年 8月.
[20] M. Yamamoto, "METI's IT Security Policy", Ministry of Economy, Trade and Industry, Japan, 2001. 6.
[21] ISO/IEC JTC 1/SC 27, "ISO/IEC 9979 Register of Cryptographic Algorithms", http://www.din.de/ni/SC27/doc7.html#9979.
[22] ISO/IEC JTC 1/SC 27, "Resolutions of the 21st Meeting of SC 27/ WG 2", ISO/IEC JTC 1/SC 27 N2720(SC 27/ WG2 N463), 2000. 10.
[23] ISO/IEC JTC 1/SC 27, "Report on the Meeting for WD 18033-3: Block Ciphers", ISO/IEC JTC 1/SC 27 N2919, 2001. 5.
[24] ISO/IEC JTC 1/SC 27, "Resolutions of the 22nd meeting of SC 27/WG 2", ISO/IEC JTC 1/SC 27/WG2 N467, May, 2001.
[25] ISO/IEC JTC 1/SC 27, "Revised Summary of National Body Comment on WD 18033-3(SC 27 N 2920) Encryption Algorithms - Part 3: Block Ciphers", ISO/IEC JTC 1/SC 27 N2975rev1, 2001. 10.
[26] ISO/IEC JTC 1/SC 27, "Disposition of Comments on WD 18033-3(SC 27 N 2920)", ISO/IEC JTC 1/SC 27 N3049, 2001. 10.
[27] 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. 10.

〈者 著 紹 介〉

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 조교수
관심분야 : 보안제품 시험, 통신망 보호, 블록암호,

차 재 현(Jae-hyeon Cha)

1985년 2월 : 한양대학교 전자계산학과 석사
2002년 2월 : 숭실대학교 컴퓨터학과 공학박사
1982년 ~ 산업자원부 기술표준원 보안기술담당관

주 학 수(Hak-Soo Ju)

1997년 8월 : 고려대학교 수학과 이학사

1999년 8월 : 고려대학교 수학과 이학석사

2001년 8월 : 고려대학교 수학과 박사과정 수료

2001년 9월~현재 : 한국정보보호진흥원 연구원

관심분야 : ECC,워터마킹,PKI

윤 선 희(Seon-Hee Yoon)

1984년 2월 : 서울대학교 자연과학대학 수학과 이학사

1986년 2월 : 서울대학교 대학원 수학과 이학석사

1995년 2월 : Univ. of Rochester 수학과 Ph. D.

2000년 2월 ~ 현재 : 한국정보보호진흥원 선임연구원

관심분야 : 블록암호, MAC

김 승 주(Seung-Joo Kim) 종신회원

1994년 2월 : 성균관대학교 정보공학과 공학사

1996년 2월 : 성균관대학교 대학원 정보공학과 공학석사 (암호학 전공)

1999년 2월 : 성균관대학교 대학원 정보공학과 공학박사 (암호학 전공)

1998년 12월 ~ 현재 : 한국정보보호진흥원(KISA) 암호기술팀장

2000년 6월 ~ 현재 : 한국정보통신기술협회(TTA) 정보통신기술위원회 암호기술연구반 의장