정 보 보 호 학 회 지
제28권 제4호, 2018. 8

ISO/IEC JTC 1/SC 27 WG2 대칭키 암호기술 국제 표준화 동향

김 동 영*, 송 정 환*

요 약

대칭키 암호기술은 고도화된 국방, 산업, 금융보안에 핵심적인 요소이다. 그리고 이에 대한 대한민국 표준기술의 국제 표준화는 그 규모가 날로 커지는 IT 산업, 금융 시장을 한국이 선도하는데 큰 도움이 된다. 본 논문에서는 국제표준화기구/국제전기표준화위원회 합동기술위원회 1/연구그룹 27 작업그룹 2(ISO/IEC JTC 1/SC 27 WG2)에서 진행되고 있는 대칭키 암호기술의 표준화 동향을 살펴본다.

Ⅰ. 서 론

2014년에 개봉한 영화 “이미테이션 게임(The Imitation Game)”은 제 2차 세계대전에서 독일군이 사용한 “애니그마” 암호장비를 통해 암호화된 통신문들을 해독하는데 천재 수학자 앨런 튜링이 기여하여 결국 연합군이 승리한다는 줄거리의 영화다. 영화에서 독일군은 암호 애니그마를 이용하여 수천 Km가 떨어진 전장에서 지령을 내려 전쟁을 수행한다. 고래로부터 적의 전략을 파악하는 것은 전쟁을 승리로 이끄는 가장 확실한 요소 중 하나이기 때문에, 연합군은 독일의 암호장비 애니그마를 획득하고 분석하여 암호화된 지령을 복호화하고 전쟁을 승리로 이끈다. 제 2차 세계대전은 그렇게 연합군의 승리로 끝이 났지만, 그 이후로 암호기술의 역할과 중요성은 더욱 높아졌다. 암호기술은 군사용뿐만 아니라 산업계에 적용되어 우리의 일상생활에 없어서는 안 될 요소가 되었다. 현재 암호기술은 우리 주변의 거의 모든 IT 기기에 적용되고 있으며, 사물인터넷(IoT, Internet of Things)의 핵심 요소가 되고, 기밀성과 무결성이 필요한 모든 정보를 안전하게 송수신 하고 있다. 암호기술의 역할이 증가한 만큼, 산업계나 금융계에서 실제로 신뢰하고 사용할 수 있는 암호기술의 표준화에 대한 요구가 증가하게 되었으며, 이에 따라 여러 형태의 암호기술에 대한 표준화가 진행되었다. 국제 표준화기구/국제전기표준화위원회 합동기술위원회 1/연구그룹 27 작업그룹 2(ISO/IEC JTC 1/SC 27 WG2, 이하 작업그룹 2)에서는 이와 같은 암호기술(cryptography and security mechanisms)에 대한 표준화를 수행하고 있다. 본 논문에서는 최근 몇 년간 작업그룹 2(WG2)에서 진행된 대칭키 암호기술에 관한 국제 표준화 동향을 살펴본다. 특히, 각국에서 이해관계에 따라 자국의 암호기술을 표준화하고, 타국의 암호기술의 표준화를 견제하는 과정을 살펴본다.

Ⅱ. 국제 표준화 동향

작업그룹 2에서 다루는 표준 목록은 [표 1]과 같다. 이 중에 대칭키 암호기술은 18033 암호 알고리즘(Encryption algorithm)에 part인 18033-3(블록암호), 18033-4(스트림암호), 29192-2(경량 블록암호), 29192-3(경량 스트림암호)가 있다. 그리고 현재 표준화되어 발간된 문서들[1,2,3,4]에 포함되어 있는 암호 알고리즘은 [표 2]와 같다. 본 단원에서는 해당 문서들에 추가될 후보로서 논의되고 있는 암호 알고리즘에 대하여 매년 2회씩 개최되는 ISO/IEC JTC SC27 회의를 기준으로 시간의 순서에 맞춰 서술한다. 앞으로 서술할 내용의 이해를 돕기 위해 암호 알고리즘이 추가되는 경우 문서의 발간 과정을 설명한다. 기존의 문서에 새로운 암호 알고리즘을 추가하려는 경우 수정본(AMD) 문서를 발간하거나 기존의 문서를 완전히 수정한다. 수정본의

* 한양대학교 수학과

개발 단계는 다음과 같다.

1. New ITEM Proposal(새로운 암호 알고리즘 제안)
2. SP(Study Period, 연구 기간)
3. WD(Working draft, 전문가 검토 단계)
4. PDAM(Proposed draft amendment, 위원회 단계)
5. DAM(Draft amendment, 승인 단계)

Simon/Speck이나 앞으로 소개할 다른 암호 알고리즘들은 수정본(AMD)을 통해 발간을 진행하고 있으므로, 위의 다섯 단계를 통하여 내용이 추가되거나, 중간 단계에서 탈락하게 된다. 1. New ITEM Proposal은 새로운 암호 알고리즘을 제안하는 단계이다. 제안된 알고리즘은 online voting을 통해 정회원국 과반수 이상이 찬성하고, 찬성한 회원국 중 분과위원회에서 활동하는 회원국이 최소 5개국이 포함되어 있으면 승인된다. 2. SP 단계는 New ITEM Proposal 단계에서 제안된 알고리즘에 대하여 선제적으로 연구, 논의하는 기간이다. 이 기간 중에 새롭게 제안되는 암호 알고리즘이 갖춰야 하는 요건에 대하여 의논된다. 대표적으로 해당 암호 알고리즘의 안전성(security), 성숙도(maturity) 등을 회원국에서 평가하고 판단한다. SP 단계에서 새로운 알고리즘이 제안되기도 한다. 3. WD 단계는 분과위원회에서 해당 암호 알고리즘 내용에 관한 표준 초안을 제작, 편집하는 과정이다. 표준 초안은 분과위원회에 상정되며, 회의 또는 online voting을 통해 분과위원회 표준안으로 상정된다. 4. PDAM 단계는 표준 초안을 분과위원회에 참여하는 회원국에 송부되고 수정되어, 회의 또는 online voting을 통해 채택되거나 폐기 또는 연기된다. 5. DAM 단계는 최종 승인 단계로서, 표준안은 투표를 통해 총회원국의 2/3 이상이 찬성하고, 투표한 회원국의 1/4 이상이 반대하지 않는 경우에 채택되어 발간된다. 앞으로 소개할 암호 알고리즘들(Simon/Speck, LEA, Kuznyechik, SM4, SKINNY, Deoxys-BC, Grain-128A, ZUC, FEA)은 이와 같은 과정을 통해 표준화 단계가 진행되고 있다.

〔표 1〕 작업 그룹 2에서 다루는 표준 목록

분류	No.	표준 제목
Encryption	18033	Encryption algorithms
	10116	Mode of operation
	29192	Lightweight cryptography
	19772	Authenticated encryption
	29150	Signcryption
Key management and hash functions	11770	Key management
	10118	Hash functions
Entity authentication	9798	Entity authentication
	20009	Anonymous entity authentication
Message authentication	9797	Message Authentication Codes (MACs)
	7064	Check character system
Non-repudiation and time-stamping	13888	Non-repudiation
	18014	Time stamping services and protocol
Digital signature	9796	Digital signature schemes giving message recovery
	14888	Digital signatures with appendix
	20008	Anonymous digital signatures
	18370	Blind digital signatures
Mathematics and cryptographic primitives	18031	Random bit generation
	18032	Prime number generation
	15946	Cryptographic techniques based on elliptic curves
	19592	Secret sharing

〔표 2〕 작업 그룹 2에서 표준화된 대칭키 암호 알고리즘

분류	No.	암호 알고리즘
블록암호	18033-3	▪ TDEA (미국) ▪ MISTY1 (일본) ▪ CAST128 (캐나다) ▪ HIGHT (한국) ▪ AES (미국) ▪ Camellia (일본) ▪ SEED (한국)
	29192-2 (경량)	▪ PRESENT (유럽) ▪ CLEFIA (일본)
스트림암호	18033-4	▪ MUGI (일본) ▪ SNOW2.0 (스웨덴) ▪ Rabbit (덴마크) ▪ Decim^{v2} (유럽) ▪ KCipher-2(K2) (일본)
	29192-3 (경량)	▪ Enocoro-128v2 (일본) ▪ Enocoro-80 (일본) ▪ Trivium (벨기에)

2.1. ISO/IEC JTC SC27 49차 멕시코 회의(2014년 10월)

미국 NSA(National Security Agency)에서 개발한 Simon/Speck을 경량 블록암호기술 표준문서에 추가하기 위하여 SP “Amendment to ISO/IEC 29192-2”를 시작하고, Simon/Speck을 후보로 제안하였다.

2.2. ISO/IEC JTC SC27 50차 말레이시아 회의(2015년 5월)

Simon/Speck은 경량암호기술로 제안되었으나, 블록길이/키 길이 쌍이 32/64, 48/72인 경우 상대적으로 짧아 안전성이 문제가 되므로 해당 파라미터를 사용하는 Simon/Speck 32/64, 48/72는 제안 문서에서 제외되었다. 그리고 Simon/Speck은 기존 18033-1[5]의 새로운 표준 알고리즘 등재 최소 요구사항을 만족하고 있으나, 독일과 벨기에 측에서 Simon/Speck의 표준화를 결정하기 전에 추가적인 안전성 증명을 위하여 SP 기간을 6개월 연장할 것을 제안하였다. 특히 벨기에 측에서 현재 Simon/Speck의 축소 라운드 공격에 관한 안전성을 검토 중이기 때문에, 해당 결과를 추가하여 6개월 뒤 회의에서 다시 논의하자고 제안하였다. 그리고 제안이 받아들여져 SP 기간이 6개월 연장되었다.

2.3. ISO/IEC JTC SC27 51차 인도 회의(2015년 10월)

지난 회의에서 독일과 벨기에 측의 요구로 SP가 연장되었으나, 향후 Simon/Speck에 관하여 추가적인 안전성 분석 결과가 없었기 때문에, 이에 근거하여 Simon/Speck의 표준화를 결정하고 SP “Amendment to ISO/IEC 29192-2”를 종료하였다. 표준화 시작 결정에 따라 Simon/Speck에 관해 ISO/IEC 29192-2\AMD1 1st WD로 초안문서가 작성되었다.

2.4. ISO/IEC JTC SC27 52차 미국 회의(2016년 4월)

독일과 벨기에 측에서 Simon/Speck의 출처가 NSA이기 때문에, Simon/Speck의 안전성을 신뢰할 수 없다고 주장하였다. 이에 대해 미국과 러시아 측에서는 암호알고리즘의 출처를 문제삼는 것은 나쁜 편견이며, 비기술적인 조건에 의하여 다른 암호 알고리즘을 제외하는 결과를 낳게 될 것이라며 우려를 표했다. 회의 현장투표를 통해 찬성 16, 기권 8 명으로 WD 단계를 연장하기로 결정하였다. (출처가 NSA인 경우 문제가 되는 이유는, NSA가 표준화된 난수발생기 Dual_EC_DRBG에 백도어를 심었다는 소문이 전 NSA 직원인 Edward Snowden에 의해 기사화되었기 때문이다.)

러시아에서 ISO/IEC 18033-3에 자국의 블록암호인 Kuznyechik을 표준화하기 위해 제안하였고, 이에 따라 SP “Inclusion of the block cipher Kuznyechik in ISO/IEC 18033-3”이 시작되었다.

2.5. ISO/IEC JTC SC27 53차 UAE 회의(2016년 10월)

Simon/Speck은 PDAM 단계로 진행되었다.

러시아의 Kuznyechik도 별 반대 없이 SP를 종료하고 ISO/IEC 18033-3/AMD1 WD 단계로 진행되었다. 한국에서 경량 블록암호 LEA를, 중국에서 블록암호 SM4를 제안하여 SP가 시작되었다. LEA의 적극적인 표준화 추진을 위해 한국의 김동찬 교수(국민대학교)가 SP의 Rapporteur를 맡았다.

2.6. ISO/IEC JTC SC27 54차 뉴질랜드 회의(2017년 4월)

Simon/Speck은 블록사이즈 128비트 미만의 Simon/Speck을 모두 제외하고 PDAM 단계에 진입했으나, 여전히 각국의 NSA에 대한 불신이 계속되었다. 이스라엘, 벨기에 측에서 NSA가 Simon/Speck의 자체 분석내용과 설계사상을 공개하고 있지 않아, 취약점 존재성에 대한 의심을 하며 표준화 진행을 극렬히 반대하고 표준화 중지를 요구하였다. 그리고 이러한 지적이 계속되자 NSA에서는 이례적으로 설계사상 문서를 작성하여 기존 문서에 추가하는 형태로 장시간에 걸쳐서 발표하였다. 이에 대한 검토를 위해 PDAM 단계를 연장하기로 결정하였다.

Kuznyechik은 반대없이 PDAM 단계로 진행되었다.

SM4의 경우 2006년부터 중국에서 사용되고 있지만, 공개된 영문 문서가 없고, AES 대비 성능 우수성 주장 미흡에 대한 지적이 있었으며, 이에 대하여 중국에서 논문 목록 및 일부 플랫폼에서의 성능 측정결과를 제시하

였다. 한국에서는 회의 전에 SM4가 일부 플랫폼에서 AES 대비 60%의 속도밖에 나오지 않는 등 (CRYPTO++ 라이브러리, PC), AES 대비 성능 우수성이 저하된다는 점을 지적했으나, 현재 LEA 표준화 진행에 있어 중국으로부터 반대 여론 형성이 될 수도 있으므로, 회의에서는 중국의 주장을 받아들이고 찬성하는 쪽으로 의견을 변경하였다. 결과적으로 중국의 SM4는 SP를 종료하고, ISO/IEC 18033-3/AMD2 WD 단계로 시작되었다.

LEA는 반대가 없어 ISO/IEC 29192-2/AMD2로 WD 단계로 시작되었다. 한국의 김동찬 교수(국민대학교)가 ISO/IEC 29192-2/AMD2의 editor를 맡았다. 전체적으로 미국을 견제하느라 러시아, 중국, 한국의 표준화 암호 알고리즘에 대한 반대여론이 강하지 않았다.

최신 대칭키 암호기술의 핵심요소나 운영 모드에 관한 의견을 받고자 SP “State-of-the-art of symmetric key primitives and related modes of operation”가 시작되었다.

2.7. ISO/IEC JTC SC27 55차 독일 회의(2017년 10월)

Simon/Speck에 대한 일부 개인연구자들을 중심으로 한 유럽 국가들로부터 지속적으로 반대의견이 개진되어 PDAM 단계를 연장하였다.

Kuznyechik은 DAM 단계를 시작하였다.

SM4와 LEA도 별 반대없이 PDAM 단계를 시작하였다.

ISO/IEC JTC SC27 54차 뉴질랜드 회의에서 SP “State-of-the-art of symmetric key primitives and related modes of operation”에 한국에서 형태보존암호의 SP를 시작할 것을 제안하였다. 이는 한국에서 개발한 형태보존암호 FEA의 표준화를 위한 사전작업이었으며, 55차 회의에서 SP “Suitability of standardization of format-preserving encryption schemes in ISO/IEC standards”가 시작되었다. FEA의 적극적인 표준화 추진을 위해 한국의 송정환 교수(한양대학교)가 형태보존암호 SP의 Rapporteur를 맡았다. 더불어 SP “State-of-the-art of symmetric key primitives and related modes of operation”에 tweak을 사용하는 tweakable 블록 암호로서 SKINNY와 Deoxys-BC가 제안되어 SP “Inclusion of SKINNY in ISO/IEC standard”와 “Inclusion of Deoxys-BC in ISO/IEC standard”가 시작되었다. SKINNY는 tweakable 블록암호이며, Deoxys-BC는 인증암호기술 공모전인 CAESAR 최종후보인 twekable 블록암호기술이다.

2.8. ISO/IEC JTC SC27 56차 중국 회의(2018년 4월)

Simon/Speck에 대하여 여전히, NSA에 대한 불신, 막연한 안전성에 대한 공방으로 표준화 진행이 지연되었다. Simon/Speck의 표준화에 관한 현장 투표(16개국가)에서 표준화 취소가 8표, 표준화 진행 4표, 기권 4표가 나왔다. 이후 총회(ISO/IEC JTC1)에서 Simon/Speck의 표준화 작업을 취소할지 진행할지에 관하여 8월 31일까지 재투표하여 최종 결정을 한다. 현재로서 Simon/Speck의 표준화 진행 가능성은 부정적이다.

Kuznyechik은 DAM 최종 승인 투표에서 21표 중에 19표 찬성, 2표 반대로 승인이 되었으므로 향후 발간될 예정이다.

SM4와 LEA는 반대없이 DAM 단계로 진행되었다.

형태보존암호에 관한 SP “Suitability of standardization of format-preserving encryption schemes in ISO/IEC standards”는 형태보존암호에 관한 의견을 더 받아들이고, 특히 형태보존암호에 관하여 양질의 의견을 받기위해 질문 내용을 구체화하자는 의견이 나와 SP 기간을 연장하였다.

스트림 암호 Grain-128a와 ZUC가 제안되어 각기 SP가 시작되었다. Grain-128a(유럽)는 eSTREAM 공모전에서 최종 단계까지 남은 Grain을 수정한 스트림 암호이며, ZUC(중국)은 3GPP에서 사용되는 스트림 암호이다.

Ⅲ. 결 론

본 논문에서는 ISO\IEC JTC 1/SC 27 WG2의 대칭키 암호 표준화 동향에 대해서 살펴보았다. 미국, 중국, 러시아, 유럽 등 각 지역에서 자국의 암호를 표준화 하거나 타국의 암호를 견제하기 위한 작업이 꾸준히 이루어지고 있다. 국내 연구자들로 구성된 한국 SC27 WG2 국내전문가 그룹에서는 충분한 안전성 분석 자료와, 각국의 이해관계를 잘 고려하여, 경량암호 LEA와 형태

보존암호 FEA의 원활한 표준화를 진행하고 있다.

참 고 문 헌

[1] ISO/IEC 18033-3:2010, "Information technology -- Security techniques -- Encryption algorithms -- Part 3:Block ciphers" 2010.

[2] ISO/IEC 18033-4:2011, "Information technology -- Security techniques -- Encryption algorithms -- Part 4:Stream ciphers" 2011.

[3] ISO/IEC 29192-2:2012, "Information technology -- Security techniques -- Lightweight cryptography -- Part 2:Block ciphers" 2012.

[4] ISO/IEC 29192-3:2012, Information technology -- Security techniques -- Lightweight cryptography -- Part 3:Stream ciphers" 2012.

[5] ISO/IEC 18033-1:2015, "Information technology -- Security techniques -- Encryption algorithms -- Part 1:General" 2015.

〈저 자 소 개〉

김 동 영 (Dong yeong Kim)

2013년 2월 : 한양대학교 수학과 졸업

2013년 3월~현재 : 한양대학교 수학과 석박사통합과정

관심분야 : 암호학, 정보보호, 블록암호

송 정 환 (Jung hwan Song)

종신회원

1984년 2월 : 한양대학교 수학과 졸업

1989년 5월 : Syracuse University 수학과 석사

1993년 5월 : Rensselaer Polytechnic Insitute 수학과 박사

1999년 3월~현재 : 한양대학교 수학과 교수

관심분야 : 암호학, 정보보호, 수리계획법