정 보 보 호 학 회 지
제25 권 제4호, 2015. 8

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

정 영 훈*, 송 정 환*

요 약

사물인터넷(IoT, Internet of Things)의 발전과 스마트 기기의 보급으로 개인정보 등과 같은 중요한 정보를 빠르고 안전하게 암호화 및 전송할 필요가 생겼다. 사물인터넷과 같이 제한된 환경에서 암호화를 할 수 있도록 설계된 암호기술을 경량 암호기술이라 한다. 본 논문에서는 국제표준화기구/국제전기표준화위원회 합동기술위원회 1 연구그룹 27 작업그룹 2(ISO/IEC JTC 1/SC 27 WG2)에서 진행되고 있는 경량 암호기술의 표준화 동향을 중심으로 우리나라의 경량 암호기술과 함께 고찰하고자 한다.

Ⅰ. 서 론

사물인터넷(IoT, Internet of Things)의 발전과 스마트 기기의 보급으로 개인정보 등과 같은 중요한 정보를 빠르고 안전하게 암호화 및 전송할 필요가 생겼다. 이때, (대칭 키, 비 대칭 키)암호 알고리즘, 해시함수, 전자서명, 인증 등 여러 가지 암호기술이 필요하다. 국제표준화기구/국제전기표준화위원회 합동기술위원회 1 연구그룹 27 작업 그룹 2(ISO/IEC JTC 1/SC 27 WG2, 이하 작업 그룹 2)에서는 이와 같은 암호기술(cryptography and security mechanisms)에 대한 표준화를 수행한다. 본 논문에서는 작업 그룹 2에서 수행 중인 표준화 동향을 살펴본다. 특히, 사물인터넷과 밀접한 연관이 있는 경량 암호기술의 표준화 동향을 자세하게 다룬다. 마지막으로 우리나라의 경량 암호기술 및 국제표준화에 대한 향후 추진 방향을 제시함으로 결론을 맺는다.

Ⅱ. 국제 표준화 동향

2.1. ISO/IEC JTC 1/SC 27 WG2 표준화 동향

ISO/IEC JTC 1/SC 27은 정보보안기술에 대한 국제표준화를 추진하고 있는 공적 표준화 연구그룹이다[1].

〔표 1〕 ISO/IEC JTC 1/SC 27의 작업 그룹

번호	작업 그룹 제목
WG 1	Information security management systems
WG 2	Cryptography and security mechanisms
WG 3	Security evaluation, testing and specification
WG 4	Security controls and services
WG 5	Identity management and privacy
SWG-T	Transversal Items
SWG-M	Special Working Group on Management

ISO/IEC JTC 1/SC 27에는 [표 1]과 같이 총 7개의 작업 그룹이 있다.

작업 그룹 2에서 다루는 표준은 [표 2]와 같다. 작업 그룹 2에서 다루는 주제로는 Encryption, key anagement and hash functions, Entity authentication, Message authentication, Non-repudiation and time-stamping, Group-based/oriented cryptography, Digital signature, Mathematic and cryptographic primitives 등이 있다. 즉, 작업 그룹 2에서는 암호기술 및 보안에 관련된 매커니즘 및 기술에 대한 표준화를 진행한다. 특히, ISO/IEC 19592 Secret Sharing는 비밀분산법에 관한 신규 표준으로 현재 Committee Draft(이하 CD)단계가 진행 중이다.

* 한양대학교 수학과 ({sky1236, camp123}@hanyang.ac.kr)

〔표 2〕 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
Group-based/ oriented cryptography	19592	Secret sharing
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

작업 그룹 2에서는 표준 등재 및 새로운 표준을 만드는 작업을 시작하기 전에 study period(이하 SP)에서 해당 안건에 대해 논의한다. 또한, 현재 암호기술 및 보안에 관련된 이슈에 대해서도 SP를 통해 논의한다. [표 3]은 현재 작업 그룹 2에서 진행 중인 SP 목록이다. 이 SP들에 대해서는 전자 문서로 의견을 제출 한 뒤, 2015년 10월에 개최되는 인도 회의에서 논의될 예정이다.

〔표 3〕 작업 그룹 2에서 진행 중인 SP 목록

SP 주제	내용
Review of UK proposal for a new mechanism in ISO/IEC 11770-3	영국이 제안한 새로운 키 합의 메커니즘의 11770-3 등재 논의
Amendment to ISO/IEC 29192-2	SIMON, SPECK의 29192-2 등재 논의
Lightweight MACs	Chaskey의 등재 논의
Privacy-respecting identity management scheme using attribute-based credentials	WG5와 공동 진행 하는 SP ; Privacy-enhanced attribute-based credential protocols의 등재 논의
Inclusion of Chinese SM2 and IBS schemes in ISO/IEC 14888-3	SM2와 IBS의 14888-3 등재 논의
Inclusion of SM3 in ISO/IEC 10118-3	SM3의 10118-3 등재 논의
Inclusion of FACE in ISO/IEC 18033-2	FACE의 18033-2 등재 논의
Quantum computing resistant cryptography	양자 컴퓨팅에 내성을 가지는 암호기술에 대한 연구
Mechanisms and properties for ISO/IEC 9798 and ISO/IEC 11770	privacy preserving authentication protocols의 등재 논의

[표 3]의 SP들 중 대부분은 신규 매커니즘 및 알고리즘의 표준 등재 논의이다. 이 알고리즘들은 이전에는 고려하지 않았던 사물인터넷 및 개인정보 보호 등을 고려하여 설계된 매커니즘 혹은 알고리즘이다. SP들 중에는 “Quantum computing resistant cryptography”와 같이 컴퓨팅의 발전 등으로 인해 향후 야기될 수 있는 문제들에 대한 사전 논의도 있다. 또한, 현재는 종료되었지만 2013년 스노우든에 의해 의문이 생긴 Dual_EC_DRBG를 SP를 통해 삭제하였다[6]. 이와 같이, 현재 작업 그룹 2에서는 암호기술에 대해 현재에서 미래까지 포괄적으로 논의하고 있다.

작업 그룹 2에서 다루는 여러 주제 중 Encryption에 해당하는 표준 및 진행상황은 [표 4]와 같다. 작업 그룹 2의 ISO/IEC 표준은 SP를 통해 논의 후 new work item proposal(이하 NWIP), Working Draft(이하 WD), Committee Draft(이하 CD), Draft International Standard(이하 DIS), Final Draft International Standard(이하 FDIS)의 과정을 거친 후 International Standard(이하 IS)로 출판된다. [표 4]의 진행상황에는

〔표 4〕 작업 그룹 2의 Encryption 주제에 대한 표준 및 진행상황

표준번호	표준 제목	진행상황	비고
18033-1	Encryption algorithms - General	2nd ed. FDIS	
18033-2	Encryption algorithms - Asymmetric ciphers	1st ed.	
18033-3	Encryption algorithms - Block ciphers	2nd ed.	SEED, HIGHT 포함
18033-4	Encryption algorithms - Stream ciphers	2nd ed.	
18033-5	Encryption algorithms - Identity-based ciphers	1st ed. DIS	신규 표준
18033-6	Encryption algorithms - Homomorphic encryption	1st ed. WD	신규 표준
10116	Modes of operation for an n-bit block cipher algorithm	4th ed. CD	
29192-1	Lightweight cryptography - General	1st ed.	
29192-2	Lightweight cryptography - Block ciphers	1st ed. AMD1 초안	
29192-3	Lightweight cryptography - Stream ciphers	1st ed.	
29192-4	Lightweight cryptography - Mechanisms using asymmetric techniques	1st ed.	
29192-5	Lightweight cryptography - Hash-functions	1st ed. DIS	신규 표준
29192-6	Lightweight cryptography - Message Authentication Codes (MACs)	1st ed. WD	신규 표준
19772	Authenticated encryption	1st ed.	
29150	Signcryption	1st ed.	

현재 표준화 중인 표준의 판 및 상태(NWIP, WD, CD, DIS, FDIS 중 하나)를 표기하였다. 진행상황에 표준화 상태가 없는 표준은 현재 표준화 작업이 이루어지지 않고 있는 것이며, 출판된 판(version)을 기재하였다. ISO/IEC 29192-2의 경우 SIMON과 SPECK 등재를 위한 개정판1(Amendment1, 이하 AMD1)의 초안이 나왔다. SP가 끝나 신규 표준으로 진행되고 있는 암호 알고리즘 관련 표준은 신원 기반 암호(ISO/IEC 18033-5), 동형 암호(ISO/IEC 18033-6), 경량 해시함수(ISO/IEC 29192-5), 경량 암호기술을 이용한 메시지 인증 코드(ISO/IEC 29192-6) 등이 있다. 이러한 표준들 역시 사물인터넷 및 빅데이터 등과 같은 기술의 발전에 의해 신규 표준으로 제정 중이다. 사물인터넷이나 빅데이터관련 기술들은 아직도 발전하고 있으며, 새로운 보안 문제점들이 나오고 있다. 작업 그룹 2에서는 이러한 사항을 반영하여 표준화를 진행하고 있다.

2.2. ISO/IEC JTC 1/SC 27 WG2 표준 알고리즘 등재 최소 요구사항

작업 그룹 2에는 총 6개의 standard document(이하 WG2 SD)가 있다. 이 중 5번째 문서인 WG2 SD5 - Process for inclusion and deletion of cryptographic mechanisms는 암호 매커니즘 및 알고리즘에 대한 표준 등재 및 삭제의 과정을 기술하고 있다. WG2 SD5문서도 SP처럼 계속 논의하여 수정되고 있다. 현재 WG2 SD5문서에 의하면 표준 등재를 위해서는 각 표준의 부록(Appendix)에 있는 최소 요구사항을 만족해야 한다고 되어 있다. 개정되지 않은 표준의 부록에는 표준에 등재 최소 요구사항이 간략하게 기술되어 있으며, 정량적이지 못하다. 실제로 ISO/IEC 18033-1:2005[2]의 부록에 비해, 현재 개정 중인 ISO/IEC 18033-1에는 등재 최소 요구사항이 자세하고 정량적으로 기술되어 있다. 개정 중인 ISO/IEC 18033-1에서의 등재 최소 요구사항은 다음과 같다.

a) Minimum key length
b) Known cryptanalysis results
c) Public domain
d) Cryptanalysis
e) Industry adoption
f) Performance

a), b), f)등은 일반적으로 암호 알고리즘 개발자들이

제안 논문을 통해 기술한다. 여기서 주목할 만한 것은 c)이다. c)의 내용은 암호 알고리즘을 public domain에 공개한지 최소 3년이 지나야 등재 제안을 할 수 있다는 것이다. 여기서 public domain이란 IACR conference나 workshop, IEEE conference, ACM conference와 같은 국제 컨퍼런스나 워크샵 혹은 ACM, Elsevier, IEEE, IEICE, SIAM, Springer와 같은 저널, 그리고 다른 국제표준 등이 있다. Public domain에 공개한지 3년이 지난 알고리즘을 그 대상으로 한 이유는 성숙도(maturity)를 위함이다. ISO/IEC 18033-1은 아직 개정 중이지만 올해 출판을 목표로 하고 있으며, 거의 마지막 단계인 DIS단계에 있다. 또한 ISO/IEC 18033은 암호 알고리즘 대한 표준으로, 최소 요구사항은 다른 표준에도 거의 동일하게 적용할 수 있다. 다른 표준들은 그 특성에 맞는 추가적인 최소 요구사항이 존재 할 수 있으나, ISO/IEC 18033-1의 최소 요구사항을 배제할 수 없다. 또한, 성숙도의 경우 대부분의 기존 표준에서는 성숙도에 대한 구체적인 기간을 제시하지 않는다. 그러나 ISO/IEC 18033-1은 c)에서 3년이라는 구체적인 기간을 제시한다. 이러한 이유로 현재 진행되고 있는 표준 등재에 관한 SP에서는 ISO/IEC 18033-1에 기재되어 있는 최소 요구사항을 고려하여 논의가 이루어지고 있다.

2.3. ISO/IEC 29192 표준화 동향

ISO/IEC 29192는 경량 암호기술(Lightweight cryptography)관련 표준이다. ISO/IEC 29192-1[4]은 경량 암호기술의 정의 등 기본적인 사항이 기술되 있으며, 나머지 파트는 알고리즘의 특성 별로 세분화 되어 있다. ISO/IEC 29192-1에 따르면 경량 암호기술은 제한된 환경에서 구현하기 위해 설계된 암호기술을 말한다. 여기서 제한된 환경이란, 하드웨어 구현 시 면적 및 전력 소비량, 소프트웨어 구현 시 프로그램 코드 크기나 필요한 메모리 크기 등이 있다. 또한, 통신 대역과 같이 상황에 따라 필요한 환경도 포함한다. 현재 경량 암호기술 관련 표준화가 진행되고 있는 SP는 “Amendment to ISO/IEC 29192-2”이다. 이는 경량 암호기술 중 블록 암호 파트인 ISO/IEC 29192-2[5]에 미국에서 제안한 SIMON과 SPECK[8]의 등재에 관한 논의를 하는 SP이다. 미국이 제시한 SIMON과 SPECK의 장점은 유연성(flexibility)과 성능(performance)이다. SIMON과 SPECK은 기존 ISO/IEC 29192-2에 등재되어 있는 표준인 PRESENT[10], CLEFIA[18]보다 다양한 종류의 블록/키 길이(32/64, 48/72, 48/96, 64/96, 64/128, 96/96, 96/144, 128/128, 128/192, 128/256 총 10종)를 지원하므로, 더 많은 환경에서 사용할 수 있다고 주장한다. 또한 ASIC, FPGA, Microcontroller, X86에서의 구현 결과를 제시하여, 하드웨어 및 소프트웨어의 성능이 PRESENT, CLEFIA보다 우수함을 강조하였다. 그러나 SIMON과 SPECK은 2013년 IACR ePrint archive에서 공개되었다. 공개된지 3년이 되지 않았으며, 공개된 곳이 저널이나 컨퍼런스가 아니다. 즉, ISO/IEC 18033-1의 최소 요구사항의 c)를 만족하지 못한다. SP논의에서 이와 같은 사항이 지적을 받았다. 미국은 SIMON과 SPECK이 공개된지 2년 반 정도 지났으며, PRESENT도 등재 논의가 될 당시에는 공개 된지 3년이 안된 알고리즘이었음을 주장하였다. 실제로 SIMON, SPECK은 등재 논의 시점에서는 공개 된지 3년이 되지 않지만, 등재가 된다면 표준화 작업 기간이 있어 등재 시점에서는 공개 된지 3년이 지난 알고리즘이 된다. 또한, IACR ePrint archive는 비록 저널은 아니지만 public domain이 될 만큼 암호 학계에서는 널리 알려진 곳이라는 주장을 하였다. 회의 후, 해당 SP의 담당자(Rapporteurs)에 의해 회의 결과가 나왔다. 해당 SP의 담당자는 미국의 의견을 수용하여 SIMON과 SPECK을 ISO/IEC 29192-2에 등재하기로 결정하였다. 하지만 최초 제안된 10종의 블록/키 길이 중 32/64와 48/72는 제외하기로 결정하였다. ISO/IEC 29192-2에 SIMON과 SPECK이 등재됨에 따라 향후 해당 표준의 AMD(Amendment)를 제정하는 표준화가 진행될 것이다.

경량 암호기술의 신규 표준으로는 경량 해시함수(ISO/IEC 29192-5)와 경량 암호기술을 이용한 메시지 인증 코드(ISO/IEC 29192-6)가 있다. ISO/IEC 29192-5는 현재 DIS단계 첫 번째 문서가 나와 있다. ISO/IEC 29192-5는 하드웨어에 최적화된 경량 해시함수와 소프트웨어에 최적화된 경량 해시함수를 구분하여 표준화 작업이 진행되고 있다. ISO/IEC 29192-5 DIS단계 첫 번째 문서에는 하드웨어에 최적화된 경량 해시함수로는 싱가포르에서 제안한 PHOTON[19], 벨기에에서 제안한 SPONGENT[9]가 포함되어 있으며, 소프트웨어에 최적화된 경량 해시함수로는 일본에서 제안한 Lesamnta-LW[14]가 포함되어 있다. ISO/IEC 29192-6은 현재

WD의 초안(preliminary draft)이 나와 있다. ISO/IEC 29192-6의 WD의 초안에는 ISO/IEC 29192-6의 전체적인 구조 및 목차만이 기술되어 있으며, 메시지 인증 코드 알고리즘은 없다.

Ⅲ. 국내 표준화 동향

ISO/IEC 표준과 부합하는 국내 표준으로는 KS X ISO/IEC 표준이 있다. KS X ISO/IEC 표준은 표준 번호 및 내용이 ISO/IEC와 일치 한다. 경량 암호기술 표준인 ISO/IEC 29192도 KS X ISO/IEC 29192로 존재한다. ISO/IEC 표준들의 최신판에 맞춰 KS X ISO/IEC 표준도 개정이 되고 있다.

3.1. 우리나라의 경량 암호기술

우리나라의 경량 암호기술로는 HIGHT[21], LEA[13], LSH[15]등이 있다. HIGHT는 암호 알고리즘 표준의 블록 암호 파트인 ISO/IEC 18033-3[3]에 SEED[22]와 함께 등재되어 있다. 또한, LEA, HIGHT, SEED는 모두 TTA표준으로 등재되어 있다[20, 21, 22]. LEA는 2013년 국가보안기술연구소에서 개발한 소프트웨어 경량 블록 암호 알고리즘이다. LEA는 ARX기반으로 32비트 플렛폼에 최적화 되어 있는 경량 블록 암호 알고리즘이다. LSH는 2014년 국가보안기술 연구소에서 개발한 경량 해시함수이다. LSH 역시 LEA와 같이 ARX기반으로 32비트 플렛폼에 최적화 되어 있는 해시함수이다.

3.2. 향후 추진 방향

3.2.1. HIGHT

HIGHT는 경량 블록 암호 알고리즘이지만 암호 알고리즘 표준의 블록 암호 파트인 ISO/IEC 18033-3에 등재되어 있다. 따라서 HIGHT를 경량 암호기술의 블록 암호 표준인 ISO/IEC 29192-2로 등재는 불가능할 것으로 사료된다.

3.2.2. LEA

LEA는 스마트그리드 보안, 모바일 기기 보안 등에서 소프트웨어 구현 및 사용을 목표로 설계된 블록 암호 알고리즘이다. 실제로 하드웨어 구현 시, AES보다 큰 면적을 차지한다.[13] 하지만 소프트웨어 구현 시, AES[11]보다 1.5 ~ 2배의 성능을 보인다.[13] 특히, ARM과 같은 모바일 환경에서 고속 암호화 및 낮은 전력소모를 가진다. 현재 ISO/IEC 29192-2에 등재된 암호 알고리즘들은 하드웨어 구현 시 효율이 높은 암호 알고리즘이 대부분이다. 이는 RFID 등 하드웨어 구현을 해야 하는 환경을 고려한 것이다. 그러나 스마트 기기의 발전 및 사물인터넷 환경을 고려하면, 특정 환경에서는 소프트웨어의 구현이 더 적합할 수 있다. 소프트웨어 구현의 장점으로는 암호 키 변경이나 암호 알고리즘 변경 등의 유지보수가 용이하다는 점이 있다. 또한, 암호 알고리즘을 라이브러리 형식으로 배포한다면 소프트웨어 개발자가 바로 사용할 수 있다는 장점도 있다. 신규 표준인 ISO/IEC 29192-5는 하드웨어에 최적화된 경량 해시함수와 소프트웨어에 최적화된 경량 해시함수를 구분하여 표준화를 진행하고 있다. 이는 ISO/IEC 29192-2에도 소프트웨어에 최적화된 경량 블록 암호 알고리즘이 필요함을 의미한다. 실제로 ISO/IEC 29192-2에 등재될 예정인 SIMON과 SPECK 중 SPECK의 경우 소프트웨어에 최적화된 경량 블록 암호 알고리즘이다. LEA는 SPECK과 마찬가지로 소프트웨어에 최적화된 경량 블록 암호 알고리즘이다. 아직까지 소프트웨어에 최적화된 경량 블록 암호 알고리즘이 SPECK 뿐 이므로 LEA도 ISO/IEC 29192-2에 등재할 수 있을 것으로 사료된다.

LEA는 2013년 WISA에서 발표되었으며, 2014년에 문서로 공개되었다. 국제 표준 등재를 추진하여, 2016년 이후 ISO에 제안 된다면 발표된지 3년이 넘게 된다. 이는 ISO/IEC 18033-1의 등재 최소 요구사항을 만족한다.

LEA가 소프트웨어에 최적화된 경량 블록 암호 알고리즘이며, 그 응용 환경 및 장점을 잘 설명한다면 ISO/IEC 29192-2에 소프트웨어에 최적화된 경량 블록 암호 알고리즘으로 제안 할 수 있을 것으로 사료된다.

3.2.3. LSH

LSH는 클라우드, 빅데이터 환경에서 대규모, 대량의 데이터등에서 소프트웨어 구현 및 사용을 목표로 설계된 경량 해시함수이다. 실제로 하드웨어 구현 시,

SHA-3(keccak)[7]보다 큰 면적을 차지한다.[15] 그러나 소프트웨어 구현 시, SHA-3대비 3배 이상의 성능을 가진다. 현재 제정 중인 ISO/IEC 29192-5의 소프트웨어에 최적화된 경량 해시함수에는 일본에서 제안한 Lesamnta-LW가 유일하다. 따라서 LSH도 ISO/IEC 29192-5에 제안 할 수 있을 것으로 사료된다.

그러나 LSH는 2014년 ICISC 2014에서 발표되었으며, 문서로 공개되었다. LSH는 현재 TTA 표준화를 진행 중이다. 즉, ISO/IEC 18033-1의 등재 최소 요구사항을 고려하면, 2017년에 제안할 수 있도록 국제 표준화를 추진해야 한다.

LSH는 ISO/IEC 29192-5에 2017년 이후에 표준화 추진이 가능하지만, 소프트웨어 구현 SHA-3대비 3배 이상의 성능을 가지는 우수한 해시함수이다. ISO/IEC 29192-5에 소프트웨어에 최적화된 경량 해시로 등재 할 수 있을 것으로 사료된다.

3.2.4. FEA

FEA[16]는 2014년 국가보안기술연구소에서 개발한 형태보존암호(format preserving encryption)이다. 형태보존암호는 입/출력 형태가 동일한 암호이다. 형태보존암호는 현재 WG2 roadmap에 포함되어 곧 표준화 작업을 진행할 암호 기술이다. FEA는 8비트 ~ 128비트의 입/출력 길이를 설정할 수 있으며, 입/출력의 길이가 동일하다. 그러나 입/출력의 길이가 동일한 것으로 모든 형태를 보존할 수 없다. 예를 들어 16자리 숫자로 이루어진 카드번호를 고려하자. 16자리 정수를 저장하기 위해서는 54비트가 필요하다. 그러나 54비트 값 중 정수로 변환 시 16자리가 넘는 정수가 나오는 값도 존재한다. 이와 같이 입/출력의 길이뿐 아니라 다른 형태도 유지할 필요한 경우 FEA는 cycle walking[17]을 이용하여 입/출력 형태가 동일하도록 한다. NIST의 형태보존암호 표준[12]의 형태보존암호들은 기존의 블록 암호 알고리즘을 이용하여 입/출력 형태를 유지할 수 있도록 하는 운영모드(mode of operation)로 동작한다. 반면, FEA는 다른 암호 알고리즘을 이용하지 않는다. 따라서 FEA는 [12]의 형태보존암호들 보다 우수한 성능을 가진다. 그러므로 형태보존암호에 대한 NWIP단계가 진행 될 때, FEA를 제안 할 수 있을 것으로 사료된다.

Ⅳ. 결 론

본 논문에서는 ISO\IEC JTC 1/SC 27 WG2의 표준화 동향에 대해서 살펴보았다. 작업 그룹 2에서는 사물인터넷, 빅데이터 등 실생활에 필요한 부분을 고려하여 표준화를 진행 중이며, 양자 컴퓨팅 등 향후 개발될 기술에도 대응 할 수 있도록 여러 논의가 진행되고 있다. 특히, 경량 암호기술 부분에 대한 표준화가 활발히 진행 중이다. 경량 해시함수와 경량 암호기술을 이한 메시지 인증 코드에 관한 표준이 새로 제정 중이며, SIMON과 SPECK는 경량 암호기술 중 블록 암호 표준에 추가로 등재 될 예정이다. 또한, 본 논문에서는 우리나라의 경량 암호기술인 LEA, LSH, FEA의 특징 및 장단점을 확인하였으며, 국제 표준 추진 방향을 제시하였다.

참 고 문 헌

[1] ISO/IEC JTC 1/SC 27 IT Security techniques, http://www.iso.org/iso/iso_technical_committee?commid=45306

[2] ISO/IEC 18033-1:2005, "Information technology -- Security techniques -- Encryption algorithms -- Part 1:General" 2005.

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

[4] ISO/IEC 29192-1:2012, "Information technology -- Security techniques -- Lightweight cryptography -- Part 1:General" 2012.

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

[6] ISO/IEC 18031:2011/Cor 1:2014, “Information technology -- Security techniques -- Random bit generation, corrigenda 1” 2014

[7] NIST, "SHA-3 Standard: Permutation-Based Hash And Extendable-Output Functions", Draft FIPS PUB 202, 2014,

[8] R. Beaulieu, D. Shors, J. Smith, S. Treatman-Clark, B. Weeks, L. Wingers, “The SIMON and SPECK Families of Lightweight Block Ciphers”, ePrint, http://eprint.iacr.

org/2013/404.pdf
[9] A. Bogdanov, M. Knezevic, G. Leander, D. Toz, K. Varıcı, I. Verbauwhede, "SPONGENT : A Lightweight Hash Function", Cryptographic Hardware and Embedded Systems - CHES 2011, LNCS 6917, pp 312-325, 2011.
[10] A. Bogdanov, L. R. Knudsen, G. Leander, C. Paar, A. Poschmann, M. J. B. Robshaw, Y. Seurin, C. Vikkelsoe, "PRESENT: An Ultra-Lightweight Block Cipher", Cryptographic Hardware and Embedded Systems - CHES 2007, LNCS 4727, pp. 450~466, 2007.
[11] J. Daemen, V. Rijmen, "The Design of Rijndael: AES - The Advanced Encryption Standard", Springer, 2002.
[12] M. Dworkin, “Recommendation for Block Cipher Modes of Operation: Methods for Format-Preserving Encryption”, NIST Special Publication 800-38G Draft, 2013.
[13] D. Hong, J. Lee, D. Kim, D. Kwon, K. Ryu, D. Lee, “LEA: A 128-Bit Block Cipher for Fast Encryption on Common Processors”, Proc. of WISA 2013, LNCS 8267, pp 3-27, 2014.
[14] S. Hirose, K. Ideguchi, H. Kuwakado, T. Owada, B. Preneel, H. Yoshida, "A Lightweight 256-Bit Hash Function for Hardware and Low-End Devices: Lesamnta-LW", Information Security and Cryptology - ICISC 2010, LNCS 6829, pp 151-168, 2011.
[15] D. Kim, D. Hong, J. Lee, W. Kim, D. Kwon, "LSH: A new fast secure hash function family", Information Security and Cryptology - ICISC 2014, LNCS 8949, pp 286~313, 2015.
[16] J. Lee, B. Koo, D. Roh, W. Kim, D. Kwon, “Format-Preserving Encryption Algorithms Using Families of Tweakable Blockciphers”, Information Security and Cryptology - ICISC 2014, LNCS 8949, pp 132-159, 2015.
[17] J. Li, C. Jia, Z. Liu, Z. Dong, “Cycle-walking revisited: consistency, security, and efficiency”, Security and Communication Networks 6(8), pp 985-992, 2013.
[18] T. Shirai, K. Shibutani, T. Akishita, S. Moriai, T. Iwata, "The 128-bit Blockcipher CLEFIA(Extended Abstract)", Fast Software Encryption, LNCS 4593, pp. 181~195, 2007.
[19] J. Guo, T. Peyrin, A. Poschmann, "The PHOTON Family of Lightweight Hash Functions", Advances in Cryptology - CRYPTO 2011, LNCS 6841, pp 222-239, 2011.
[20] 박제홍, 홍득조, 김동찬, 권대성, 박해룡, “128비트 블록암호 LEA”, TTAK.KO-12.0223, December 2013.
[21] 전길수, 이상진, 염용진, 박해룡, 김현, “64비트 블록암호 HIGHT”, TTAK.KO-12.0040/R1, December 2008.
[22] 전길수, 이향진, 김지연, 박해룡, 주학수, “128비트 블록암호 알고리즘 SEED”, TTAS.KO-12.0004/R1, December 2005.

〈저자소개〉

정 영 훈 (Young hoon Jung)
2011년 2월 : 한양대학교 수학과 졸업
2011년 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