정 보 보 호 학 회 지
제 33 권 제4호, 2023. 8

ISO/IEC JTC 1 SC 27 암호기술 국제표준화 동향

권 대 성*

요 약

암호기술 국제표준화는 각국의 국가표준기구들이 가입된 ISO/IEC의 JTC 1 산하 SC 27 내 WG(Working Group) 2에서 진행되고 있다. 현재 70여 편의 암호기술 표준이 제정되어 있으며, 최근에는 양자컴퓨터 위협에 대응하기 위한 양자내성 공개키암호와 전자서명, 데이터 보안에 활용할 수 있는 완전동형암호 및 다자간 안전계산의 표준화가 주를 이루고 있다, 본 고에서는 전체적인 표준화 현황을 간략하게 살펴보고, 최신 이슈가 되고 있는 표준화 현황에 관해 설명한다.

Ⅰ. 서 론

암호기술 표준화는 적용된 암호기술의 상호 연동성을 확보하고자 하는 일반적인 표준화의 목적부터 시작된다. 그런데, 암호기술은 저장/통신 데이터 및 관련 서비스의 안전성을 보장하는 기술이므로, 잘못된 구현을 방지할 수 정밀한 규격이 제공되어야 하며, 표준화된 암호기술 자체도 안전해야 한다.

국제 표준화는 암호기술을 널리 사용하기 위한 목적을 가지고 있으며, 용도별로 안전성 및 성능을 고려하여 선정하는 원칙을 가지고 있다.

암호기술은 단독으로 사용되기 보다는 다양한 프로토콜/서비스에 적용되어 사용되는데, 국제 표준은 이런 사용에 있어 기반이 된다.

대표적인 암호기술 국제표준은 ISO/IEC 표준이다. 각 국가의 국가표준기구들이(한국의 경우 국가기술표준원) 가입된 국제 표준기구 ISO, IEC가 ICT 표준화를 위하여 연합하여 설립한 JTC 1(Joint Technical Committee 1) 산하의 SC 27(SubCommittee 27) 내의 WG 2(Working Group 2)에서 암호기술 표준화 작업을 진행하고 있다.

현재, 암호기술은 블록 암호, 공개키 암호 등 암호화 알고리즘을 비롯하여 70여 종이 표준으로 제정되어 있으며, 새로운 ICT 적용, 새로운 보안기능의 필요에 따라, 신규 암호기술 표준화가 제안되고 있다.

제2절에서는 현재 제정되어 있는 표준들에 대해서 주요 표준들 중심으로 살펴보고, 제3절에서는 최근 이슈가 되고 있는 양자내성 암호기술, 완전 동형암호, 다자간 안전계산 기술들의 표준화 동향에 대해서 살펴본다.

Ⅱ. ISO/IEC 암호기술 표준화 현황

이 절에서는 ISO/IEC의 주요 표준들의 현황을 살펴본다.

가장 전통적이기도 하고 많은 부분을 차지하고 있는 암호화 알고리즘을 먼저 살펴보자. 암호화 알고리즘은 ISO/IEC 18033 암호화 알고리즘(Encryption algorithms)과 ISO/IEC 29192 경량암호(Lightweight cryptography)로 나뉘어져있다. 특히, 한국에서 개발한 일반 블록암호 SEED, HIGHT가 18033에, 경량 블록암호 LEA가 29192에 포함되어 있다. 암호화 알고리즘은 암호기술 표준화에서 가장 관심이 높은 분야이며, 의견 충돌이 가장 많은 분야이기도 하다.

2.1. 범용 암호화 알고리즘 표준화

암호화 알고리즘의 대표적인 표준인 ISO/IEC 18033은 공개키암호, 블록암호, 스트림암호, ID기반 암호, 동형암호, 트윅가능 블록암호, 완전동형암호 등 8개 Part로 구성되어 있다[표 1].

현재 많은 표준들이 제정되어 있으며, 한편에서는 일부 사용이 적은 표준들을 폐지하자는 의견들이 있었으며, 이에 대한 절차를 만드는 작업도 진행되었으나, 일부 산업체에서 적용되고 있다는 논리들로, 폐지는 거의 이루어지지 않았다.

* ETRI 부설연구소 (책임연구원, ds_kwon@nsr.re.kr)

〔표 1〕 ISO/IEC 18033 표준 현황

Part	제정/ Edition	내용
Part 1: 일반	2021년/ 제3판	알고리즘 요건 등
Part 2: 비대칭키 암호(공개키 암호)	2006년/ 제1판	ECIES-KEM, PSEC-KEM, ACE-KEM, RSAES, RSA-KEM, HIME(R), HC
	2017년/ AMD 1	FACE-KEM
	AMD 2 (착수)	CRYSTALS-Kyber, FRODO-KEM, Classic McEliece
Part 3: 블록암호	2010년/ 제2판	64-bit: TDEA, MISTY1, CAST-128, HIGHT: 128-bit: AES, Camellia, SEED.
	2021년/ AMD 1	SM4
Part 4: 스트림암호	2011년/ 제2판	MUGI, SNOW 2.0, Rabbit, Decimv2, KCipher-2 (K2)
	2020년/ AMD 1	ZUC
Part 5: ID기반 암호	2015년/ 제1판	BF, SK, BB1
	2021년/ AMD 1	SM9
Part 6: 동형암호	2019년/ 제1판	Exponential ElGamal, Paillier
Part 7: 트윅가능 블록암호	2022년/ 제1판	Deoxys-TBC, Skinny
Part 8: 완전동형암호		새로운 표준으로 작업 예정

최근에는 러시아에서 제안한 블록암호 Kuznyechik의 표준화 과정에서 논란이 있었다. 이 블록암호의 설계자들은 구성요소 중 하나인 S-box를 랜덤하게 생성하였다고 주장하였는데, 랜덤하게 생성된 S-box가 가지기 힘든 성질이 발견되었다. 비록 이 성질을 이용한 직접적인 공격이 발견되지는 않았지만 블록암호의 안전성에 대해 의문을 제기하는 전문가들이 많아졌고, 결국 표준화를 중단하는 것으로 의결하였다. 이는 안전성에 대한 의혹이 있으면 표준화가 어렵다는 것을 잘 보여주고 있다.

표준들의 특성은 공개키 암호의 경우, 주요 용도인 키암호화에 맞게 표준들이 제안되었다는 것과, 최근 미국 NIST의 PQC 공모사업 선정 결과 및 안전성 리포트를 근거로 새로운 공개키 암호의 표준화가 착수되었다는 것이다. 이 부분은 다음 절에서 다시 다루고자 한다.

[표 1]에서 보면 AMD(Amendment)는 기존 문서에 알고리즘을 추가하기 위한 표준화 작업으로 보면 되는데, 프로젝트의 part별로 최대 2편까지만 허용된다.

그리고, [표 1]에서 완전동형암호가 Part 8로 구성되어 표준화가 진행되고 있는데, 표준화 착수 시 설정한 기한을 맞추기 어려워서 새로운 프로젝트로 다시 시작하기 위한 작업이 진행 중에 있다,

표준 제안 시 국가별로 차이점이 있는데, 중국과 러시아는 자국 국가표준 암호기술을 자국 시장에서 널리 사용하고 있다는 이유로 제안하고 있으며, 이 외 국가들에서는 기존 암호기술과의 차별성, 우수성을 고려하여 표준을 제안하고 있다.

중국 제안 블록암호 SM4와 표준화가 좌절된 러시아의 Kuznyechik가 암호 자체의 우수성은 떨어지지만, 규모가 큰 자국 시장에서의 활용을 앞세워 표준화를 추진한 경우이다.

2.2. 경량 암호기술 표준화

다음으로 경량 암호 표준이다. 경량 암호를 어떻게 정의할 수 있는가는 논란의 소지가 많이 있다. 자원이 제약된 기기에서의 구현에 적합한 암호기술이라고 하고는 있지만 범용 암호도 구현 범위가 넓게 개발되고 있을 뿐만 아니라 소형 기기들도 자원제약 문제를 해소하고 있기 때문이다.

경량 암호 표준 ISO/IEC 29192는 블록 암호, 스트림암호, 비대칭키 기법 기반 메커니즘, 해시 함수, MAC, 브로드캐스트 인증 프로토콜, 인증 암호화로 구성되어 있다. 기존 암호화 알고리즘 표준과는 구성의 차이가 있다. 해시 함수, MAC, 인증 암호화는 별도 표준으로 제정되어 있는데, ISO/IEC 29192는 이러한 표준들의 경량 버전들을 다루고 있다고 보면 된다.

한국 개발 알고리즘이 18033-3에 포함될 때는, 알고리즘 우수성보다는 한국의 국가표준이라는 명분을

내세웠는데, 경량 블록암호 LEA의 경우에는 경량암호 국제 구현 프로젝트에서 해당 부분 1위를 한 실적을 기반으로 알고리즘의 우수성을 내세워 경량 블록암호 부분에 포함되었다.

경량 암호 표준 ISO/IEC 29192의 표준현황 및 포함 메커니즘을 정리하면 [표 2]와 같다.

경량 암호 표준화에서 논란이 있었던 부분은 경량 블록 암호다. 한국의 경량 블록암호 LEA보다 조금 일찍 시작된 미국 NSA가 제안한 SIMON, SPECK 블록 암호에 대한 논쟁이다. 두 블록암호의 표준화 과정에서 논란이 된 부분은 안전성에 대한 NSA 능력과 의혹이라고도 볼 수 있다. 스노든 폭로에서 드러난 난수발생기 백도어처럼 NSA가 해독할 수 있는 암호를 표준화하는 것이 아니냐는 의혹으로 지리한 논쟁 끝에 두 블록 암호의 표준화는 좌절되었다.

이 과정에서 검토되었던 또 한 부분은 블록 암호의 블록 크기이다. 현재는 주로 64비트와 128비트의 블록암호를 사용하고 있다. 하지만 최근 대부분의 경량 환경에서 128비트 블록 암호를 수용할 수 있으므로, 짧은 키 갱신 주기로 인한 취약점이 발생할 수 있는 64비트 블록 암호는 향후 표준화 대상에서 제외하자는 의견이 많이 있었다. 이러한 사항은 앞으로 블록암호 표준화에 영향을 미칠 가능성이 있다.

〔표 2〕 ISO/IEC 29192 표준 현황

Part	제정/Edition	내용
Part 1: 일반	2012년/제1판	정의 알고리즘 요건 등
	AMD 1 (착수)	하위 part 설명 추가
Part 2: 블록암호	2019년/2판	PRESENT, CLEFIA, LEA
Part 3: 스트림 암호	2012년/제1판	Enocoro, Trivium
Part 4: 비대칭 기법 기반 메커니즘 (인증,서명)	2013년/제1판	cryptoGPS, ALIKE ID기반 서명
	AMD 1/2016년	ELLI
Part 5: 해시 함수	2016년/제1판	PHOTON, SPONGENT, Lesamnta-LW
Part 6: 메시지 인증코드(MAC)	2019년/제1판	LightMAC, Tsudik's keymode, Chaskey-12
Part 7: 브로드캐스트 인증 프로토콜	2019년/제1판	TESLA-RD
Part 8:인증 암호화	2022년/제1판	Grain-128A

2.3. 난수발생기 표준화

그리고, 또 하나 관심을 받는 표준은 ISO/IEC 18031 난수발생기 표준이다. 이 표준은 앞에서 언급했던 스노든의 폭로로 밝혀진 NSA 백도어 표준이 포함되었던 표준이다. 2011년에 제정된 표준에는 이와 더불어 여러 표준이 포함되어 있었다. 난수발생기 표준에서 seed를 기반으로 결정적으로 난수를 생성하는 DRBG(Deterministic Random Bit Generator) 알고리즘 들인데, 해시 함수 기반 DRBG, 블록 암호 기반 DRBG, 정수론 난제 기반 DRBG, 다변수 2차 방정식 기반 DRBG 등이 있다. 이 중에서 NSA가 제안한 방식이 Dual_EC_DRBG, MS_DRBG 이다.

Dual_EC_DRBG는 스노든의 폭로로 사용이 제한되었지만(2017년 발간된 AMD 1에서 Dual_EC_DRBG의 사용 제한), 여전히 본 표준에서 제거되지 않았었는데, 난수발생기 표준의 시험/검증과의 통일성을 위한 개정을 추진하면서(현재 진행 중), 일부 의혹이 있거나 안전성 이슈가 있는 MS_DRBG와 MQ_DRBG도 함께 제외하기로 의결하였다.

난수발생기는 암호키를 만드는 방법으로 충분한 난수성이 확보되어야 하고, 생성된 난수 간에도 충분한 독립성이 확보되어야 한다. 그리고 난수를 생성하는 방법도 위의 결정론적인 방법과 비결정론적인 방법도 있어, 이를 시험/평가하는 방법과도 통일성을 확보해야 하는 필요성이 있다. 현재 이를 반영한 표준 개정 작업이 진행되고 있다.

ISO/IEC에는 앞에서 설명한 표준 외에도 많은 표

〔표 3〕 ISO/IEC 18031 표준

표준	제정/개정	포함된 알고리즘
18031	2011년	hash_DRBG, HMAC_DRBG CTR_DRBG OFB_DRBG Dual_EC_DRBG MS_DRBG MQ_DRBG

〔표 4〕 ISO/IEC WG2 표준 현황

프로젝트	표준
18033	Encryption algorithms
29192	Lightweight cryptography
10116	Mode of operation for an n-bit block cipher
10118	hash functions
9797	Message authentication codes
19772	Authenticated encryption
14888	Digital signatures with appendix
9796	Digital signatures giving message recovery
13888	Non-repudiation
9798	Entity authentication
18031	Random bit generation
18032	Prime number generation
15946	Cryptographic techniques based on elliptic curves
11770	Key management
29150	Signcryption
23264	Redaction of authentic data
20008	Anonymous digital signatures
20009	Anonymous entity authentication
18370	Blind digital signatures
18014	Time-stamping services
7064	Check character systems
19592	Secret sharing
4922	Secure multiparty computation

준이 제정되어 있다. 표준들을 프로젝트별로 분류해 보면 [표 4]와 같다. 프로젝트의 세부 파트에 대한 기술은 생략한다. 각 파트가 독립적 표준이며, 현재 70여 편의 표준이 존재한다. 새로운 ICT 보안 요구에 따라 새로운 표준이 지속해서 제안되고 있으며, 사용되지 않는 표준은 많지는 않지만 폐지되고 있다.

Ⅲ. ISO/IEC 암호기술 최근 표준화 동향

제2절에서는 암호기술 주요 표준화 현황을 살펴보았는데, 제3절에서는 최근 이슈가 되고 있는 표준화 현황에 대해서 살펴본다,

최근 암호기술 표준화에서 이슈가 되는 것은 다음과 같다.

- 양자컴퓨터 위협에 대응하기 위한 (공개키, 전자서명) 암호기술 표준화
- 머신 러닝 등에서 데이터 프라이버시에 활용할 수 있는 완전동형암호 표준화
- 개인의 데이터를 제공하지 않으면서, 다자간에 연산을 수행하는 다자간 안전계산 표준화

3.1. 양자컴퓨터 위협 대응을 위한 암호기술 표준화

양자컴퓨팅에서 Shor 알고리즘을 이용하면 기존 공개키 암호의 주를 이루는 인수분해, 이산대수 기반 공개키암호를 매우 짧은 시간에 해독할 수 있다는 것이 알려져 있다.

미국 NSA에서는 2015년 공개키암호를 PQC로 전환하는 계획을 발표하였으며, NIST에서는 양자컴퓨터 위협에 대응하기 위하여 2016년 기존의 표준 공개키 암호를 대체하기 위한 PQC 공모사업을 시작하여 2022년 7월에 4개의 선정 암호를 발표하였다.

키교환/암호화에 CRYSTALS-Kyber 1종, 전자서명에 CRYSTALS-Dilithium, Falcon, SPHINCS+ 3종을 선정하고, 추가 선정을 위한 4라운드 후보로 키교환/암호화에 Classical McEliese, BIKE, HQC, SIKE 등 4종을 포함하고, 전자서명은 추가 공모사업을 진행하고 있다.

WG 2는 NIST 공모사업이 진행되는 도중에, NIST 공모사업에 협력하고 공모사업 이후 표준화를 진행하고자, 2020년 양자내성암호에 대한 이해를 돕기 위한 기술 현황 분석을 기술 분야별로 공개 기술 문서(standing document)로 공개하였다.

〔표 5〕 WG 2 양자내성암호 기술분석 문서(SD8)

구분	프로젝트 명
Part 1	General post-quantum & motivation
Part 2	해시 함수 기반 전자서명(Hash-based signatures)
Part 3	격자 기반 암호(Lattice-based cyptography)
Part 4	코드 기반 암호(Coding-based encryption)
Part 5	다변수 기반 전자서명(Multivariate-based signatures)
Part 6	이소지니 기반 암호(Isogeny-based encryption)

PQC 기술 중 개발 후 안전성이 충분히 검증된 해시함수 기반 전자 서명에 대해서 우선적인 표준화가 진행 중이다.

현재 ISO/IEC 표준화가 추진되고 있는 전자서명의 경우, 안전성이 해시함수의 안전성에만 의존하는 것이 명확한 구조로, 양자컴퓨터에 대한 안전성을 보장하지만 일반적인 목적으로 사용하는 데는 한계가 있다. 그렇지만, 공모사업이 종료되기 전이거나, 공모사업이 종료되더라도 선정된 암호들에 대한 의문이 있을 경우에도, 안전성에 대한 신뢰를 가지고 우선 적용할 수 있는 전자서명이다.

ISO/IEC의 양자컴퓨팅에 안전한 전자서명 표준화는 별도 분류가 아닌 전자서명의 한 부분으로 진행되고 있다. ISO/IEC의 전자서명 프로젝트는 14888(부가형 전자서명, Digital signatures with appendix)이다. 참고로 Part 3 이산로그 기반 전자서명에는 한국에서 개발한 KCDSA, EC-KCDSA가 포함되어 있다.

NIST의 PQC 공모사업에서 2022년 7월에 1차 선정 결과가 발표되었는데, 애초에는 NIST의 표준화가 종료된 후, ISO/IEC 표준화를 진행될 예정이었다.

그런데 2022년 가을 회의에서 독일이 NIST 공모사업에서 선정되지는 않았지만, 공모사업을 통하여 안전성이 충분히 검증되었고 유럽에서 이미 적용되기 시작한 FRODO-KEM의 표준화를 제안하였다. 비록 NIST의 표준화가 종료되지는 않았지만 많은 전문가가 표준화 추진에 찬성하여 양자내성 KEM의 표준화 논의를 시작하기로 의결하였다. 이 과정에서 FRODO-KEM뿐만 아니라 NIST 공모사업에서 선정된 CRYSTALS-Kyber와 4라운드에 포함된 Classic McEliece의 표준화도 함께 논의하기로 결정하였다.

2023년 봄 회의에서 6개월간의 의견 수렴 결과를 종합하여 양자내성 KEM의 표준화를 착수하는 것으로 결정되었다.

해당 표준화를 새로운 프로젝트로 추진할 것인지, 기존 표준에 알고리즘을 추가하는 형태인 AMD로 추진할 것인지에 대한 논의가 진행되었는데, PQC-KEM은 기존 표준(ISO/IEC 18033-2) 범주에 속하므로, 기존 표준의 AMD로 추진하는 것으로 결정되었다([표 1] 참조).

ISO/IEC에서 암묵적으로 협의가 이뤄진 것은 NIST 공모사업 또는 이에 준하는 검증 절차로 안전성이 충분히 검증된 암호 알고리즘만 표준화의 대상으로 논의하겠다는 것이다.

그리고, 양자컴퓨팅 위협에 대한 안전성을 제공하는 PQC는 공개키 암호/전자 서명 알고리즘에 추가된 안전성을 제공하는 암호기술이므로 기존 공개키 암호/전자 서명 분야에서 표준화를 진행한다는 것이다.

현재는 양자컴퓨터에 대한 안전성을 제공한다는 것이 공개키 암호/전자 서명에 대한 추가적인 안전성 요구사항으로 받아들여지고 있지만, 앞으로는 암호기술에 대한 기본적인 안전성 요구사항이 되어야 할 것이다.

이런 관점에서 보면, 현재 존재하는 많은 응용 전자서명, 인증, 프로토콜 기술들이 대체되거나, 사용이 제한되어야 하며, 이를 위한 기술개발 및 표준개발이 수반되어야 할 것이다.

〔표 6〕 전자서명(ISO/IEC 14888) 표준 현황

Part	제정/ Edition	알고리즘
Part 1: 일반	2008년/ 제2판	
Part 2: 인수분해 기반	2008년/ 제2판	GQ1, RSA, RW, ESIGN, GQ2, GPS1,GPS2
Part 3: 이산로그 기반	2018년/ 제4판	DSA, KCDSA, Pointcheval/Vaudeney, SDSA, EC-DSA, EC-KCDSA, EC-GDSA, EC-RDSA, EC-SDSA, EC-FSDSA, SM2, IBS-1, IBS-2
Part 4: Stateful 해시함수 기반	진행 중	XMSS, LMS, $XMSS^{MT}$, HSS

3.2. 완전동형암호 표준화 현황

완전동형암호 표준화에 앞서 동형암호 표준화가 2014년부터 시작되었다. 동형암호 표준화의 대상이 된 알고리즘은 덧셈 또는 곱셈 등 한 가지 연산에 대해서 암호문 연산이, 평문 연산 후 암호화한 결과와 같은 성질을 가져 부분 동형암호라고 부르기도 하며, 2000년 이전에 개발되었으나, 활용도가 명확하지 않아 표준화는 추진되지 않았다.

그런데, GDPR 제정 등으로 프라이버시 보호 필요성이 증가하면서, 데이터 활용과 프라이버시 보호라

는 두 가지 목적을 달성하는 완전 동형암호(모든 연산 가능)가 2009년부터 본격적으로 발표되기 시작하였다.

그러나, 완전 동형암호를 적용하기에는 많은 자원이 필요로 하는 등의 제약이 있어, 기존에 개발된 (부분)동형암호 표준화가 2014년에 시작되어, 2019년에 완료되었다([표 1] 참조).

완전 동형암호 표준은 IBM을 중심으로 개발이 시작되었으며, 현재는 4개의 알고리즘(BFV, BGV, CKKS, CGGI)의 표준화가 추진되고 있다. 4개의 알고리즘 모두 개발자의 첫 글자를 딴 명칭을 사용하고 있다. 이 중 CKKS는 한국에서 개발한 알고리즘이다.

BFV/BGV는 2009년 IBM의 Gentry가 발표한 완전 동형암호 기술을 발전시킨 암호화 기법이다. CKKS는 암호문에 연산을 수행하면 연산된 평문으로 정확하게 복호화되지 않고, 근삿값으로 복호화된다. 하지만 이러한 성질로 인해 효율성이 높아 머신러닝 등에 사용할 수 있다는 특성이 있다.

완전 동형암호를 사용하기 위한 라이브러리들이 다수 개발되었으며, 완전 동형암호 개발자들의 표준화 홈페이지[4]에서 확인할 수 있다.

완전 동형암호의 ISO/IEC 표준화는 2020년에 공식 제안되었고, 암호화 알고리즘의 Part 8로 진행하는 것으로 결정되었다([표 1] 참조).

그런데, 코로나로 인하여 표준화 회의가 온라인으로 열려 타 전문가들과 소통이 활발하게 이루어지지 않아, 표준화 진행이 원활하게 되지 않았다. 결국 2023년 봄 회의에서 표준화 기한 제약으로 기존 표준화(ISO/IEC 18033-8) 진행은 중단하고, 새로운 프로젝트로 추진하는 것으로 결정되었다.

완전 동형암호는 Bootstrapping, packing, batching 등 성능을 향상시키는 세부 기술들이 계속 개발되고 있어 표준화를 어떻게 진행할 것인가에 대한 논의사항들이 여전히 남아있다.

표준화를 하는 목적은 해당 기술을 산업에 적용하고자 하는 것인데, 표준은 구형 기술이고, 제품에 적용하는 라이브러리는 신형기술로 차이가 존재하면, 표준의 의미가 퇴색될 뿐만 아니라, 추후 시험/검증 시에 표준을 중심으로 할 수밖에 없어, 신형기술에 대한 시험이 이루어지기 어려운 점도 존재한다.

완전 동형암호 프로젝트는 새로운 프로젝트 번호를 부여받을 예정이며, 알고리즘별로 Part를 구성해서 추진할 계획이다. 알고리즘별로 별도 표준이 되는 것이며, 표준화 진행도 알고리즘별로 진행될 수 있어 표준화 완료 시점에도 차이가 발생할 수도 있다.

3.3. 다자간 안전계산 표준화 현황

다자간 안전계산 기술은 다수의 사용자가 본인의 정보를 다른 사용자에게 공개하지 않고 다수의 정보를 입력으로 하는 함수를 계산하는 기술이다.

동형암호와 차이점은 동형암호는 암호화된 결과값을 제공하지만 다자간 안전계산은 여러 사용자가 본인 데이터 제공없이 프로토콜을 통하여 사용자들의 데이터들에 대한 연산을 수행한다는 면에서 차이가 있다.

동형암호는 기기에서의 연산 처리, 다자간 협업 등의 어려움이 관건이라면, 다자간 안전계산 기술은 프로토콜 통신량이 관건이 되는 기술이라고 할 수 있다.

다자간 안전계산 기술은 20년 넘게 연구되었으나 활용도가 낮았다. 그러나 동형암호와 마찬가지로 데이터 보안 필요성으로 인하여, 최근 산업화를 하고 있는 기술이다.

산업화가 추진됨에 따라, ISO/IEC 표준화도 진행되고 있다([표 7]).

다자간 안전계산 중 가장 간단한 형태가 비밀분산 기법을 활용하는 방식이다. 비밀분산기법은 별도의 프로젝트로 2017년에 표준화가 완료되었다(ISO/IEC 19592).

비밀분산 기법에 기반한 다자간 안전계산 표준에서는 ISO/IEC 19592의 비밀분산 기법 중 Shamir, Replicated additive를 주로 이용하며, 이를 이용하여 덧셈, 뺄셈, 곱셈 등을 다자간에 안전하게 할 수 있는 프로토콜을 제시하고 있다.

Garbled circuit 기반 다자간 안전계산 표준화는 Garbled circuit을 별도 표준화를 하지 않고 해당 표

〔표 7〕 다자간 안전계산(ISO/IEC 4922) 표준 현황

Part	제정	알고리즘
Part 1: 일반	2023년	
Part 2: 비밀분산기반	진행 중	ISO/IEC 19592 비밀분산기법 기반
Part 3: Garbled circuit 기반	진행 예정	free XOR, half gates 포함, 추가 기법 포함 예정

〔표 8〕 비밀 분산(ISO/IEC 19592) 표준 현황

Part	제정	알고리즘
Part 1: 일반	2016년	
Part 2: 비밀분산	2017년	Shamir, Ramp Shamir, Additive, Replicated additive, Computational additive

준에 포함하여 진행하는 것으로 결정되었다.

우선 표준화 대상 circuit으로 보안 요소가 적은 free XOR, half gates를 우선 추진하기로 하였으며, 추가 메커니즘 포함을 위한 논의를 병행하여 진행하기로 하였다. Garble circuit에 많이 활용되는 OT(Oblivious Transfer)를 black-box로 하는 표준화를 추진하려고 하였으나, 표준은 입력에 대한 출력을 얻는 메커니즘 구현을 비전문가가 할 수 있도록 제시하는 규격이므로 이러한 접근은 불가하다는 의견이 많은 상황이다.

안전한 다자계산은 아직 실용화 초기 단계이며, 현재 기술도 많은 프로토콜 통신량으로 인하여 적용에 어려움이 존재한다.

국내에서도 데이터 보호 필요성으로 인하여, 이러한 기술개발 소요가 향후 발생할 것으로 예상되고 있다. 오랫동안 이론 연구가 진행되었지만, 실용화 단계로 접어들고 있어 실용 관점에서의 연구개발 및 표준화도 중요한 시기로 접어들고 있다.

Ⅳ. 결 론

암호기술의 핵심 국제표준화기구인 ISO/IEC JTC 1/SC 27에서의 표준화 현황을 살펴보았다. 암호기술 표준화는 오랜 기간동안 진행되어 왔으며, 다양한 ICT 보안 요구에 대응하기 위하여 70여 편의 표준이 제정되어 있으며, 최근에는 양자컴퓨터에 대응하기위한 공개키 암호/전자서명, 데이터 프라이버시 이슈를 대응하기 위한 동형암호, 다자간 안전계산 기술 중심으로 표준화가 진행되고 있다.

국내 개발 암호기술이 블록 암호, 전자 서명, 완전 동형암호 표준으로 제정되었거나, 표준화가 추진 중이다.

최근에는 중국, 러시아를 제외하면, ISO/IEC는 국가 표준이라는 사유라기 보다는 암호 기술의 우수성을 내세워 표준화가 진행되고 있다.

암호기술이 널리 활용되기 위해서는 ISO/IEC 표준으로 제정되는 것이 가장 큰 출발점이라고 할 수 있다.

국내에서도 널리 활용될 수 있는 암호 기술을 확보하기 위해서는 최근 이슈가 되는 분야에서 우수성을 인정받는 기술을 확보하기 위한 노력이 진행될 필요가 있을 것이다.

참 고 문 헌

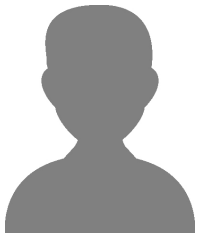
[1] 권대성, “양자컴퓨터 위협 대응을 위한 양자내성암호와 양자암호”, *TTA 저널*, 206호, pp. 56-73, 2023.

[2] ISO/IEC JTC 1/SC 27 Information security, cybersecurity and privacy protection 홈페이지, “https://www.iso.org/committee/45306.html”.

[3] NIST Post-quatum cryptography 홈페이지, “https://csrc.nist.gov/projects/post-quantum-cryptography”.

[4] Homomorphic Encryption Standardization Home page, “https://homomorphicencryption.org/”.

〈저 자 소 개〉



권 대 성 (Daesung Kwon)
정회원
1992년 2월 : 서울대 수학과 졸업
1994년 2월 : 서울대 수학과 석사
1999년 2월 : 서울대 수학과 박사
2001년 3월~현재 : ETRI 부설연구소 책임연구원
<관심분야> 암호, 정보보호, 양자암호