1915호
2019.09.25.
ISSN 1225-6447

Weekly ICT Trends

주간기술동향

IITP 정보통신기획평가원

Weekly ICT Trends
주간기술동향 1915호
ISSN 1225-6447

chapter 1

차세대 표준암호기술 동향

노동영 ‖ 국가보안기술연구소 선임연구원
권대성 ‖ 국가보안기술연구소 센터장

미국 NIST와 국제표준화기구 ISO/IEC, ITU-T 등은 현 암호시스템에 대한 양자컴퓨터의 위협에 대응하기 위해 양자내성 공개키 암호(Post Quantum Cryotography: PQC)와 양자키 분배(Quantum Key Distribution: QKD) 기술에 대한 표준화를 추진하고 있다. 그리고 ISO/IEC는 초연결 환경에서 데이터의 신뢰성 제공을 위한 경량 암호 표준체계를 갖추어 가고 있다. 본 고에서는 양자내성 공개키 암호, 양자키 분배 기술의 소개와 표준화 진행 현황을 살펴보고자 한다. 그리고 SW 환경에서 최고 성능을 지닌 국내 블록암호 LEA의 ISO/IEC 경량 암호 분야 표준화가 2019년 말 완료될 예정임에 따라, 미국의 표준화 실패 사례 등과 비교하여 체계적으로 준비가 되었던 LEA의 개발 및 표준화 과정을 소개하고자 한다.

I. 서론

4차 산업혁명 시대에 접어들면서 다양하게 생성·유통되는 정보의 보호, 자동화된 기기의 제어 안전성 확보, 다양화·소형화된 디바이스의 보안, 개인정보 보호의 필요성이 증가하고 있는데, 가장 기반이 되는 것은 암호기술이다. 고대로부터 우리 생활의 안전과 매우 밀접한 관계가 있었던 암호기술은 현대에 들어서는 해독기술의 발전 및 요구조건의 고도

* 본 내용은 노동영 선임연구원(☎ 042-870-4786, dyroh@nsr.re.kr)에게 문의하시기 바랍니다.
** 본 내용은 필자의 주관적인 의견이며 IITP의 공식적인 입장이 아님을 밝힙니다.

화로, 안전하면서도 성능이 좋은 암호기술의 개발은 매우 어렵고 도전적인 과제가 되었다. 뿐만 아니라, ICT 및 정보보안 시장이 글로벌화됨에 따라 암호기술에 대한 국제 표준화의 필요성도 증가하고 있다. 암호기술 국제 표준화는 미국, 유럽 등이 주도하고 있었으나, 최근에는 중국의 약진이 눈에 띄고 있다.

현재 연구/개발 및 표준화가 가장 활발한 암호기술 분야는 미국 NIST가[1] 공모사업을 진행하고 있는 양자컴퓨팅에 안전한 공개키 암호, 도청에 대한 완벽한 물리적 안전성 제공이 가능한 양자키 분배 기술과 초연결 시대에서 요구되고 있는 경량 암호기술이다.

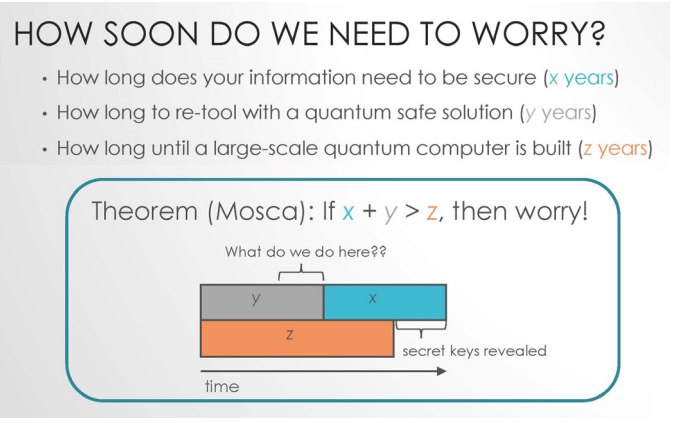
본 고에서는 앞서 언급한 세 암호기술 분야에 대해 간단히 설명하고, 관련 표준기술 동향을 살펴보고자 한다. II장에서는 양자 내성 공개키 암호, III장에서는 양자키 분배 기술, IV장에서는 경량 암호기술을 설명하고, 표준화 동향을 살펴본다. 마지막으로 V장에서 본 고의 결론을 제시한다.

II. 양자내성 공개키 암호

현재 가장 널리 사용되는 공개키 암호로는 RSA(Rivest-Shamir-Adleman, 1977), ECC (Elliptic Curve Cryptography, 타원곡선암호, 1985)를 들 수 있다. 이들은 소인수 분해 또는 이산 로그 문제라는 수학적 난제에 안전성의 기반을 두고 있다. 하지만 양자컴퓨터가 개발되면 소인수 분해 및 이산 로그 문제는 다항식 시간 내에 해결이 가능해 현 공개키 암호들이 더 이상 안전하지 않게 된다. 이러한 이유로 양자컴퓨터에 안전한 수학적 난제 및 이를 이용한 공개키 암호의 개발이 활발하게 진행되고 있으며, 이를 표준화하기 위한 작업도 동반되고 있다. 앞서 언급한 양자컴퓨팅에 안전한 공개키 암호는 양자내성 암호 또는 Post Quantum Cryptography(PQC)로 부르고 있다.

양자컴퓨터를 이용한 현 공개키 암호의 해독에는 아직 많은 시간이 남아 있다고 예상되지만, PQC의 개발 및 표준화는 지금부터 준비해야 한다. 캐나다 양자컴퓨팅 분야 전문가 모스카의 부등식(Mosca's inequality)에서 보듯이 암호기술은 개발 후 적용에 걸리는 기간 및 데이터 보호가 필요한 기간을 고려하였을 때, 해독기술이 본격화되기 수년 전에

1) 미국 국립표준기술연구소(National Institute of Standards and Technology)



〈자료〉 "The ship has sailed," Dustin Moody, 2017.

[그림 1] 모스카의 부등식

개발 및 표준화가 완료되어야 하기 때문이다([그림 1] 참조).

PQC에 대한 구체적 논의는 2006년 PQCrypto 학회가 시작되면서 본격화되었다. 하지만 기술 개발은 1970년대 후반 부호기반 공개키 암호 McEliece 및 해시함수 기반 Lamport, Merkle 전자서명, 2000년대 초 격자기반 공개키 암호 NTRU 등 이미 오래전부터 연구/개발되고 있었다. 현재도 연구/개발이 매우 활발하며, 최근에는 PQC의 구현 테스트도 다방면으로 이루어지고 있다. 예를 들어, Microsoft는 PKI에 전자서명 PICNIC을 구현하였고, 키교환 알고리즘 NewHope은 구글의 인터넷 브라우저 크롬 및 인피니언 비접촉 보안칩에 구현되었다.

NIST에서는 양자컴퓨터 위협에 대응하여, 2016년 기존의 표준 공개키 암호를 대체하기 위한 PQC 공모사업을 시작하였다.

1라운드 평가대상 접수는 2017년 12월까지 이루어졌는데, 전 세계적으로 69개의 후보가 제출되었다. 우리나라에서도 5개를 학계, 연구소 등이 제안하였다. 후보들은 기반을 두는 문제 특성에 따라 격자(lattice), 코드(code), 다변수(MP), 해시(hash), 타원곡선(isogeny)의 5종으로 분류 가능하며, 기능별로는 암호화/키교환, 전자서명 2종으로 분류할 수 있다. 주로 안전성 관점에서 1라운드 후보들에 대한 평가가 진행되었고, 2019년 1월에 26개의 2라운드 후보를 선정하였다([표 1] 참조). 아시아에서는 중국이 제안한 1개의 알고리즘만 2라운드 후보에 포함되었고, 미국, 프랑스, 네덜란드에서 제안한 알고리즘

들이 주를 이루었다. 2라운드에서는 안전성과 더불어 성능평가가 이루어질 예정이다. 최종 표준 선정은 안전성/효율성 등의 공개 검증을 위해 3~5년 정도 걸릴 것으로 예상된다.

NIST 공모사업과 더불어 국제표준화 기구인 ISO(International Organization for

[표 1] NIST PQC 표준화 프로젝트 2라운드 선정 공개키 암호

알고리즘 명	대표 저자	대표 기관	대표 국가	기반문제	기능
BIKE	R. Misoczki	Intel	미국	Code	암호화/키교환
Classic McEliece	D. J. Bernstein	University of Illinois	미국	Code	암호화/키교환
CRYSTALS-KYBER	P. Schwabe	Radboud University	네델란드	Lattice	암호화/키교환
FrodoKEM	M. Naehrig	Microsoft	미국	Lattice	암호화/키교환
HQC	P. Gaborit	University of Limoges	프랑스	Code	암호화/키교환
LAC	X. Lu	Chinese Academy of Sciences	중국	Lattice	암호화/키교환
LEDAcrypt	M. Baldi	Universit`a Politecnica delle Marche	이탈리아	Code	암호화/키교환
NewHope	T. Poppelmann	Infineon Technologies AG	독일	Lattice	암호화/키교환
NTRU	Z. Zhang	Onboard Security	미국	Lattice	암호화/키교환
NTRU Prime	D. J. Bernstein	University of Illinois	미국	Lattice	암호화/키교환
NTS-KEM	M. Albrecht	Royal Holloway Univ. of London	영국	Code	암호화/키교환
ROLLO	P. Gaborit	University of Limoges	프랑스	Code	암호화/키교환
Round5	O. Garcia-Morchon	Phillips	네델란드	Lattice	암호화/키교환
RQC	P. Gaborit	University of Limoges	프랑스	Code	암호화/키교환
SABER	F. Vercauteren	KU Leuven	벨기에	Lattice	암호화/키교환
SIKE	D. Jao	University of Waterloo	캐나다	ETC	암호화/키교환
Three Bears	M. Hamburg	Rambus	미국	Lattice	암호화/키교환
CRYSTALS-DILITHIUM	V. Lyubashevsky	IBM Zurich	스위스	Lattice	전자서명
FALCON	T. Prest	Thales Commun. & Security	프랑스	Lattice	전자서명
GeMSS	L. Perret	Sorbonne Universities	프랑스	MP	전자서명
LUOV	W. Beullens	KU Leuven	벨기에	MP	전자서명
MQDSS	S. Samardjiska	Radboud University	네델란드	MP	전자서명
Picnic	G. Zaverucha	Microsoft	미국	Hash	전자서명
qTESLA	N. Bindel	TU Darmstadt	독일	Lattice	전자서명
Rainbow	J. Ding	University of Cincinnati	미국	MP	전자서명
SPHINCS+	A. Hulsing	Eindhoven Univ. of Technology	네델란드	Hash	전자서명

〈자료〉 국가보안기술연구소 자체 작성

Standardization)/IEC(International Electrotechnical Commission)도 PQC에 대한 지속적인 논의를 하고 있다. JTC 1/SC 27/WG 2에서는[2] 다양한 PQC 알고리즘에 대한 조사 및 표준화 준비를 위해 공개 기술 문서인 standing document를 작성 중이다(SD8, [표 2] 참조)[4]. 최근 회의에서는 기술 현황에 대한 기술발표를 진행하고 있으며, 본격적인 표준화는 NIST 공모사업이 완료된 후에 진행될 것으로 예상된다. 다만, PQC 기술 중 개발 후 충분한 검증기간을 가졌던 해시함수 기반 전자 서명에 대해서는 우선적인 표준화가 진행될 예정이다.

PQC 개발 및 표준화의 가장 큰 숙제는 “양자컴퓨터에 대한 안전성을 어떻게 검증하는가?”이다. 아직 고성능의 양자컴퓨터가 개발되지 않았기 때문에 PQC의 안전성 기반이 되는 수학적 난제들을 해결할 수 있는 양자 알고리즘을 비롯하여 양자 인공지능을 이용한 문제 해결 방법 등에 더 많은 연구와 시간이 필요하다. 결과에 따라 PQC 알고리즘 개발은 변화의 여지가 남아 있으며, 보안에 적용하기 위한 규격 완성 및 표준화 등도 상당기간이 소요되고 많은 변화를 동반할 것으로 예상된다.

[표 2] ISO/IEC JTC 1/SC 27/WG 2 SD8 세부 프로젝트 개발 현황

연번	프로젝트 명	비고
Part 1	General post-quantum & motivation	draft posted
Part 2	Hash-based signatures	draft posted
Part 3	Lattice-based cyptography	draft posted
Part 4	Coding-based encryption	draft posted
Part 5	Multivariate-based signatures	under development
Part 6	Isogeny-based encryption	draft posted

〈자료〉 국가보안기술연구소 자체 작성

III. 양자키 분배

양자키 분배는 에너지의 최소 단위인 양자(量子, Quantum)를 이용하여 암호키를 전달하는 기술이다. 이 기술의 특징은 기존 공개키 암호나 PQC와 같이 수학적 난제에 기반을

2) Information security, cybersecurity and privacy protection - Cryptography and security mechanisms

두지 않고 불확정성의 원리(Uncertainty Principle), 복제 불가능 정리(No Cloning Theorem) 등 양자물리학의 기본 가정에 기반을 두고 안전성을 보장한다는 것이다. 특히, 양자컴퓨터, 슈퍼컴퓨터 등 컴퓨팅 능력이 발전되어도 안전성이 저하되지 않고, 컴퓨터를 활용한 문제해결 알고리즘 능력의 발전과도 무관하여 장기간 사용하여도 안전성이 저하되지 않는 장점을 가지고 있다.

양자 암호키 분배 기술은 1984년 Bennett과 Brassard가 양자를 이용하여 안전하게 암호키를 분배하는 프로토콜을 발표하면서 시작되었다[6]. 두 사람이 제안한 프로토콜은 BB84라 불리며, 현재에도 가장 많이 활용되고 있다.

양자키 분배기술은 현재 IDQ(스위스), Toshiba(일본), MagiQ(미국), Quantum CTek(중국), SKT 등 다양한 회사에서 상용화 혹은 상용화 준비를 진행하고 있다([표 3] 참조). 상용화 기술은 단일광자 사용의 어려움을 극복하기 위해 고안된 디코이 적용 BB84 프로토콜을 구현한 시스템이 대부분이며, 대체적으로 50km 내외의 전송거리에서 최적 키생성률이 제시되고 있다.

[표 3] 주요 회사의 양자키 분배 시스템

회사명	Toshiba	IDQ	NEC	QAsky	Quantum CTek	SKT
Key Rate	13.72Mbps @10km	1.42kbps @50km	112.4kbps @22km	40kbps @50km	50kbps @50km	10kbps @50km
Key Rate@50km	2.17Mbps	1.42kbps	40kbps	40kbps	50kbps	10kbps
Protocol	Decoyed BB84	COW	Decoyed BB84	Decoyed BB84	Decoyed BB84	Decoyed BB84
Encoding	Phase	Time-bin	Phase	Phase	Polarization	Phase

〈자료〉 Toshiba (2017 ETSI Quantum Workshop 발표)

그런데, 이 기술의 구현 문제는 ① 일정한 간격으로 단일광 생성 ② 수신 디바이스의 감지 오류 ③ 광원의 도달거리(상용 광통신망 약 100km 내외) 등으로 좁혀질 수 있다. 이러한 문제를 해결하기 위한 기술 개발이 지금도 진행 중이다.

양자키 분배는 상기 구현 한계에 따른 문제들과 더불어 암호시스템 공격기술인 각종 물리적/SW적, 지능적 공격 등에 대해서도 충분한 검토가 요구된다.

양자키 분배 표준화에 대한 검토를 앞서서 진행한 곳은 유럽 표준협회인 ETSI(European Telecommunications Standards Institute, 유럽전기통신표준협회)이다. ETSI는 양자

[표 4] 양자키 분배 관련 ETSI 출판물

출판명	제목
ETSI GS QKD 012 V1.1.1	Quantum Key Distribution(QKD): Device and Communication Channel Parameters for QKD Deployment
ETSI GS QKD 014 V1.1.1	Quantum Key Distribution(QKD): Protocol and data format of REST-based key delivery API
ETSI GR QKD 007 v1.1.1	Quantum Key Distribution(QKD): Vocabulary
ETSI GR QKD 003 v2.1.1	Quantum Key Distribution(QKD): Components and Internal Interfaces
ETSI GS QKD 011 V1.1.1	Quantum Key Distribution(QKD): Components characterization: characterizing optical components for QKD systems
ETSI GS QKD 005 V1.1.1	Quantum Key Distribution(QKD): Security Proofs
ETSI GS QKD 008 V1.1.1	Quantum Key Distribution(QKD): QKD Module Security Specification
ETSI GS QKD 004 V1.1.1	Quantum Key Distribution(QKD): Application Interface
ETSI GS QKD 002 V1.1.1	Quantum Key Distribution(QKD): Use Cases

〈자료〉 국가보안기술연구소 자체 작성

키 분배 위원회를 두고 있으며, 7개의 GS(Group Specification)와 2개의 GR(Group Report)을 출판하고 갱신하고 있다([표 4] 참조).

국내에서는 TTA(Telecommunications Technology Association, 한국정보통신기술협회)에서 표준화를 진행하고 있는데, 통신망 기술위원회(TC2)에서는 ETSI 문서 도입 표준을, 정보보호 기술위원회(TC5)에서는 국가공공 도입에 필요한 프로토콜 규격과 보안 요구사항을 독자적으로 개발하고 있다([표 5] 참조).

[표 5] 양자키 분배 관련 TTA 표준화

표준번호	표준명
TTAK.KO-12.0329-Part1	양자키분배: 제 1부: 일반
TTAK.KO-12.0329-Part2	양자키분배: 제 2부: BB84 프로토콜
2019년 출판예정	양자키분배: 보안요구사항
TTAE.ET-GS QKD 008	양자키분배: 모듈보안규격
TTAE.ET-GS QKD 011	양자키분배: 구성요소특성화: QKD시스템의 광학구성요소 특성화
TTAE.ET-GS QKD 004	양자키 분배망: 응용 인터페이스
TTAE.ET-GS QKD 003	양자키분배: 구성요소 및 내부인터페이스

〈자료〉 국가보안기술연구소 자체 작성

ISO/IEC에서는 중국이 표준화 추진에 앞장서고 있다. 암호키 분배 관련 표준은 TTA 표준에서처럼 크게 두 가지로 분류된다. 프로토콜 동작 규격을 정하는 암호 알고리즘과 이를 암호모듈에서 안전하게 운용하기 위한 보안 요구사항(또는 평가기준)으로 나뉜다. 일반적인 표준화 절차는 암호 프로토콜(알고리즘) 표준화가 선행된다. 그러나 ISO/IEC의 암호 알고리즘 표준화 그룹에서는 이를 지지하고 있지 않아서, 중국 등은 규격이 명시되지 않은 평가 기준 표준화만을 추진하고 있다. 2017년 가을 독일 회의에서 표준화 추진이 제안되었고, 2019년 봄 이스라엘 회의에서 정식 표준화 과제로 채택되었다([표 6] 참조).

[표 6] 양자키 분배 관련 ISO/IEC JTC 1/SC 27 표준화

프로젝트 번호	제목
23837-1	Security requirements, test and evaluation method for qkd-Part 1. Requirements
23837-2	Security requirements, test and evaluation method for qkd-Part 2. Test and evaluation methods

〈자료〉 국가보안기술연구소 자체 작성

한편, ITU-T에서는 양자키 분배 활용 및 양자난수발생기 구조에 대한 다양한 표준화를 SG13과 SG17에서 진행하고 있다. ITU-T의 국제표준화는 KT(SG13) 및 SKT(SG17)가 문서개발 주관을 맡아 표준화 활동을 주도하고 있다([표 7] 참조).

[표 7] 양자키 분배 관련 ITU-T 표준화 추진 현황

프로젝트 번호	제목
Y.3800	Framework for networks supporting QKD
Y.QKDN_SDNC	Software Defined Network Control for Quantum Key Distribution Networks
Y.QKDN_Arch	Functional architecture of the Quantum Key Distribution Network
Y.QKDN_KM	Key management for Quantum Key Distribution Network
Y.QKDN_CM	Control and Management for Quantum Key Distribution Network
X.cf-QKDN	Use of cryptographic functions on a key generated in QKD networks
X.qrng-a	Quantum noise random number generator architecture for consent
TR.sec-qkd	Technical report on security framework for quantum key distribution in telecom network
X.sec-QKDN-km	Security requirements for quantum key distribution networks - key management
X.sec-QKDN-ov	Security requirements for quantum key distribution networks - overview
X,5Gsec-q	Security guidelines for applying quantum-safe algorithms in 5G systems

〈자료〉 국가보안기술연구소 자체 작성

ISO/IEC 표준화는 프로토콜을 특정하지 않는 평가방법을 대상으로 하고 있어 보안성 검토에 한계가 있을 것으로 보이며, ITU-T 표준화는 다양한 의견 제기 단계이다.

암호키 분배는 암호시스템에 있어서 핵심적인 안전성을 제공하는 요소이므로, 충분한 검토 및 객관적 신뢰성 확보가 필요한 부분이다. 암호키 분배의 취약점은 정보시스템 전체의 붕괴로 연결될 수도 있기 때문에, 암호를 주도하고 있는 미국 등에서 양자키 분배의 표준화에 신중을 기하고 있다.

IV. 경량 암호

기존 암호화 알고리즘 분야에서는 경량 암호가 최근 이슈가 되고 있다. 초연결 시대가 도래하면서 데이터를 더 작은 기기에서 더 빠르게 암호화해야 할 필요성이 대두되고 있다. ISO/IEC에서는 제법 오래전부터 경량 암호를 하나의 분야로 지정하여 표준화를 하고 있다[2]. 경량 암호 표준은 다양한 부분으로 나뉘어 있는데([표 8] 참조), 가장 논의가 치열하고 기술 집약적인 부분이 블록암호 분야이다[3]. 기존 표준으로는 유럽의 PRESENT와 일본의 CLEFIA가 있는데 활용도는 크지 않다.

이 분야의 가장 큰 변화는 미국 NSA(National Security Agency, 미국 국가안보국)가 2013년 두 개의 경량 블록암호 SIMON/SPECK[5]을 발표하면서 이루어졌다. 특히, SIMON/SPECK은 기존 어떤 블록암호들보다 우수한 경량성을 보유하고 있을 뿐만 아니라, NSA

[표 8] ISO/IEC 경량 암호 분야(ISO/IEC 29192-Lightweight cryptography) 세부 프로젝트

프로젝트 연번	프로젝트 명	비고
29192-1	General	-
29192-2	Block ciphers	LEA 포함 추진 중
29192-3	Stream ciphers	-
29192-4	Mechanisms using asymmetric techniques	-
29192-5	Hash-functions	-
29192-6	Message authentication codes (MACs)	개발 중
29192-7	Broadcast authentication protocols	개발 중
29192-8	Authenticated encryption	개발 중

〈자료〉 국가보안기술연구소 자체 작성

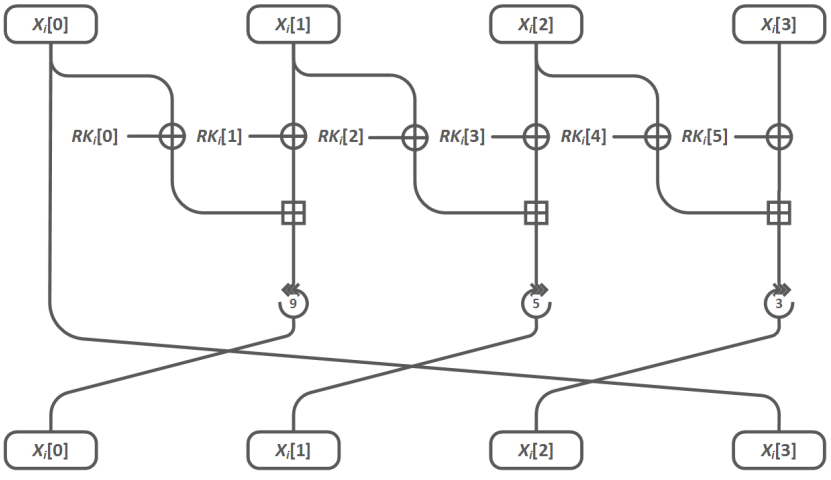
가 처음으로 공개적으로 개발한 암호 알고리즘이어서 많은 관심을 받았다.

미국은 2016년 두 암호를 ISO/IEC 암호기술 그룹에 제출하였다. 그러나 2013년 스노든의 폭로로 밝혀진 백도어의 여파가 거셌다. 기존에는 미국이 제안한 암호들은 쉽게 ISO/IEC 표준으로 채택되는 분위기였는데, NSA에서 제안한 난수발생기 표준에 백도어 삽입 의혹이 발표되면서 분위기가 반전되었다.

표준화 회의에 참석한 많은 전문가들이 지속적으로 설계에 대한 투명성 문제를 제기하였다. 미국이 이에 대해 해명을 하였음에도 불구하고 2018년 봄 중국 회의에서 표준화 추진 취소 절차가 시작되었다. 그 후 국가 단위 투표를 통해 2018년 8월 최종적으로 표준화 추진 취소가 확정되었다.

국내에서는 IoT 환경에 적합한 암호화 기술 확보를 목적으로 2014년에 개발된 고속 경량 블록암호 LEA(Lightweight Encryption Algorithm)[7]를 2016년 미국에 이어 경량 블록암호 표준으로 제안하였다. LEA는 SW에서의 최적 속도를 위해 매우 간단한 구조(덧셈, 비트순환, XOR 만으로 연산)를 채택하였다([그림 2] 참조).

LEA는 2015년 룩셈부르크대학 개발 경량암호 성능 측정 프레임워크 FELICS[8]를 활용한 구현경진대회에서 128비트 블록암호 부분 1위를 차지하는 등 경량 소프트웨어 환경에서의 성능 우수성이 검증되었다. 특히, 현재 가장 널리 사용되는 국제표준 블록암호 AES 대비 1.5배 이상의 속도를 제공한다.



〈자료〉 국가보안기술연구소 자체 작성

[그림 2] 경량 고속 블록암호 LEA

[표 9] LEA의 ISO/IEC 표준화 추진 현황

시기	추진 현황
2016년 10월, UAE 회의	LEA 표준화 제안 및 사전 연구 단계(study period) 시작
2017년 4월, 뉴질랜드 회의	문서 작성 단계(Working Draft: WD) 시작
2017년 10월, 독일 회의	위원회 검토 단계(Committee Draft: CD) 시작
2018년 4월, 중국 회의	표준 초안 단계(DIS, draft international standard) 시작
2019년 4월 이스라엘 회의	표준 승인 단계(FDIS, final draft international standard) 시작
2019년 10월~11월	표준화 완료 예정, LEA가 포함된 ISO/IEC 29192-2:2019 출판 예정

〈자료〉 국가보안기술연구소 자체 작성

LEA와 SIMON/SPECK은 유사한 구조를 가지고 있으며, 모두 IoT 환경에서 우수한 성능을 가지고 있다. 하지만 LEA의 경우 안전한 설계로 인한 견고한 안전성, AES 개발기관이자 유럽에서 암호관련 R&D를 선도하고 있는 벨기에 루벤대학 등 제 3자에 의한 객관적 안전성 평가, 철저한 표준화 준비로 큰 이견 없이 2019년 말 ISO/IEC 경량 블록암호 표준으로 제정될 예정이다([표 9] 참조).

한편, ISO/IEC 일반 블록암호 표준에는 우리나라 블록암호 SEED와 HIGHT가 포함되어있다[1]. 하지만 SEED와 HIGHT는 국제표준 AES 대비 낮은 성능으로 인하여 암호제품의 국제 경쟁력 확보에는 한계가 있다. 반면, LEA는 우수한 SW 성능으로, 국내에서는 SW 중심의 보안제품이 대부분을 차지하고 있는 만큼 그 활용도도 크다고 할 수 있다.

V. 결론

본 고에서는 차세대 표준암호기술 동향을 살펴보았다. 구체적으로 최근 가장 이슈가 되고 있는 양자컴퓨팅에 안전한 공개키 암호, 양자키 분배 기술, 경량 암호기술의 표준화 동향을 살펴보았다.

양자컴퓨터의 위협에 대응하기 위해 양자컴퓨팅에 취약한 기존 공개키 암호를 PQC로 대체하기 위한 개발 및 표준화가 활발히 진행 중이다. 하지만 아직 양자 알고리즘에 대한 이해가 부족하여 앞으로 개발 및 안정화에 많은 시간이 걸릴 것으로 예상되며, 많은 변화를 동반할 것으로 예상된다.

양자적 특성을 이용한 양자키 분배에 대한 표준화도 꾸준히 진행 중이다. 비록 키분배라는 한정적인 기능 밖에 제공하지 못하지만, 물리적으로 완벽히 안전한 키분배를 달성할 수 있기에 많은 관심을 받고 있다. 하지만 아직 키분배 가능 거리, 구현 과정에서 발생할 수 있는 각종 오류 및 공격에 대한 연구가 더 필요하다.

마지막으로 초연결 시대에 필요한 경량 암호 역시 표준화가 활발히 진행 중이다. 특히, 암호화에 가장 기본이 되는 블록암호 분야의 연구 및 표준화에 많은 역량이 집중되고 있다. 우리나라는 체계적인 준비과정을 거쳐 국내 개발 경량 고속 블록암호 LEA를 ISO/IEC 국제 표준으로 추진 중에 있으며, 2019년 말에 경량 블록암호 표준으로 등록될 예정이다.

앞으로도 암호기술의 표준화에 대한 수요는 증가할 것으로 보이며, 우리나라도 그에 발맞추어 지속적인 연구/개발 및 표준화를 위한 노력이 필요하다.

[참고문헌]

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

[2] “Information technology -- Security techniques -- Lightweight cryptography,” ISO/IEC 29192.

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

[4] “ISO/IEC JTC 1/SC 27/WG 2 SD8 - Post-Quantum Cryptography,” 2019.

[5] R. Beaulieu, D. Shors, J. Smith, S. Treatman-Clark, B. Weeks, L. Wingers, “The simon and speck families of lightweight block ciphers,” Cryptology ePrint Archive, 2013/404, 2013.

[6] C.H. Bennett, G. Brassard, “Quamtum cryptogrphay: public key distribution and coin tossing,” IEEE International conference on computers, systems & signal processing, 1984, pp.175-179.

[7] D. Hong, J.K. Lee, D.C. Kim, D. Kwon, G.H. Ryu, D. Lee, “LEA: A 128-bit Block Cipher for Fast Encryption on Common Processors,” WISA 2013, Lecture Notes in Computer Science, volume 8267, 2014, pp.3-27.

[8] FELICS(Fair Evaluation of Lightweight Cryptographic Systems), https://www.cryptolux.org/index.php/FELICS.

chapter 2

양자컴퓨터 R&D 현황과 전망

이준 ‖ 한국과학기술정보연구원 책임연구원

I. 서론

양자컴퓨터에 대한 발상은 미국 칼텍(Caltech)의 이론물리학자인 리처드 파인만(Richard Feynman) 교수가 1981년 로스 알라모스 연구소에서 행한 강연에서 양자병렬성을 이용하여 기존 컴퓨터로는 계산이 불가능한 문제를 양자역학기반 전산시스템으로 해결할 수 있을 것이라고 발표한 제안[5]을 그 출발점으로 받아들이는 것이 일반적이다. 이어 1985년에는 영국의 데이비드 도이치(David Deutsch) 교수가 이론적으로 양자 상태를 응용한 데이터 처리가 가능함을 입증한 논문을 발표[1]하였고, 1994년 미국 AT&T 벨연구소의 피터 쇼어(Peter Shor)는 최초의 양자 알고리즘을 제시[4]하면서 양자컴퓨터에 대한 본격적인 연구 개발이 시작되었다. 양자컴퓨터란 양자역학의 주요 원리 및 양자현상에 따라 구현되고 작동되는 새로운 개념의 컴퓨터로 정보처리의 기본단위로 양자비트(Qubit, 이하 큐비트)를 사용한다. 큐비트는 기존 컴퓨터에서는 구현 불가능한 상태인 '0'이면서 동시에 '1'도 될 수 있는 중첩(superposition) 현상과 양자상태에서 어떤 한 계의 상태가 측정을 통해 결정됨에 따라 그 계와 얽혀 있는 다른 계의 상태 또한 순간적으로 결정된다는 얽힘(entanglement) 현상 등을 기반으로 작동한다. 이를 통해 기존 컴퓨터가 특정 입력에

* 본 내용은 이준 책임연구원(☎ 042-869-0675, rjlee98@kisti.re.kr)에게 문의하시기 바랍니다.
** 본 내용은 필자의 주관적인 의견이며 IITP의 공식적인 입장이 아님을 밝힙니다.

[표 1] 양자컴퓨터 활용이 기대되는 분야

분야	응용 예	사례	분야	응용 예	사례
금융	- 포트폴리오 최적화 - 리스크 관리 - 옵션가격 결정	- 2016년, D-Wave Systems와 1QBit가 "Quantum for Quants" 설립	물류	- 비행기, 선박, 트럭 등의 물류 최적화	- PLC와 Manchester Met. 대학의 물류 알고리즘 공동 개발
화학	- 분자 설계 최적화 - 화학 반응의 양자 역학적 시뮬레이션 - 전지와 촉매의 최적화	- IonQ의 화학 시뮬레이션 SW 개발 - MS의 기초 연구 - ETH, Harvard대학 등의 연구 등	제약	- 단백질의 3차원 구조 최적화/분석 (알츠하이머병 등 특효약 개발)	- Stanford대학의 "Folding@home" 프로젝트 - Harvard대학/D-Wave Systems의 단백질 분석 실험
의료	- 암 치료용 약물 발견/최적 복용량 산출 - 개인 맞춤형 의료의 고속화	- Stanford대학, Texas대학에서 연구	자동차	- 도시 교통 서비스 최적화	- Volkswagen과 Google의 공동 개발 - Volkswagen의 주문형 이동 서비스를 위한 알고리즘 개발
IT	- 머신 러닝을 위한 고속 클러스터링 - 이미지 인식 고속 학습	- Google/D-Wave Systems의 이미지 인식 정확도 향상 - (중) USTC, NMR 기술 이용 4 큐비트 양자 프로세서 개발	항공 우주	- 유체 역학적으로 최적화된 기체 설계 - 비행 제어 시스템의 버그 잡기 최적화	- NASA의 비행체 날개 설계 최적화 - Lockheed Martin과 Airbus의 제어 시스템 버그 탐색 SW 개발 (6개월 → 6주)

〈자료〉 量子コンピュータの最新動向(MaMasayuki Minato, GREE ventures, 2018.1.), IITP(2018.2.)에서 재인용

대응하는 유일한 결과만 생성하는 반면, 양자컴퓨터는 이와 같은 양자 특성을 이용하여 구성하고 있는 큐비트가 적은 경우에도 많은 경우의 수를 동시 다발적으로 표현할 수 있을 뿐만 아니라, 큐비트의 비결정론적 특성을 이용하여 여러 결과를 동시에 생성할 수 있다는 장점을 지닌다.

[표 1]에서는 양자컴퓨터가 이와 같은 기존 컴퓨터 대비 월등한 연산속도를 바탕으로 기존 산업에 미칠 것으로 예상되는 분야를 예시하였다[3],[15]. 이와 같은 맥락에서 본고는 양자컴퓨터의 출현 배경이 된 기존 컴퓨터 관련 주요 이슈를 살펴보는 한편, 양자컴퓨터 개발을 둘러싸고 세계 주요 선진국이 주도권을 잡기 위해 노력하고 있는 양자컴퓨터의 핵심기술 개발 현황과 국내외 양자컴퓨터 관련 주요 정책, 주요 기업별 개발 동향과 향후 전망에 대해 살펴보고자 한다.

이를 위해 먼저 II장에서는 양자컴퓨터의 출현 배경이 된 기존 반도체 집적화 기술의 한계 및 경제성 상실, 에너지 효율에 대한 대안 모색 등의 관점에서 이슈를 살펴보고 양자

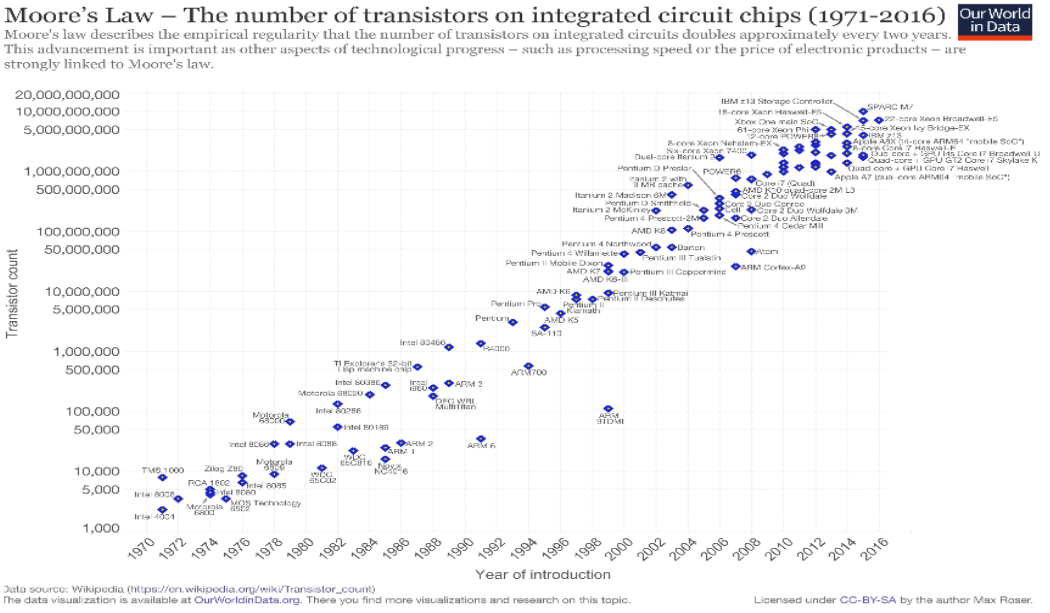
컴퓨터의 기반이 되는 주요 요소 기술 관련 기술개발 동향을 살펴보는 한편, 양자컴퓨터 기술의 현주소를 파악하고자 하였다. 이어 III장에서는 양자컴퓨터 생태계 조성을 위해 추진하고 있는 관련 정책을 국가 차원에서 소개하는 한편, 양자컴퓨터 개발을 주도하는 선도 기업 사례를 소개함으로써 양자컴퓨터 도래에 따른 기대 효과를 확인해 보고, 마지막으로 IV장에서 본 고의 결론을 제시하였다.

II. 기존 컴퓨터의 주요 이슈 및 양자컴퓨터 기술 개발 현황

1. 기존 컴퓨터 관련 주요 이슈

가. 반도체 집적 공정을 둘러싼 이슈

최근 들어 무어의 법칙으로[1] 대변되는 반도체 미세공정이 정체기에 이르자 많은 전문가들은 반도체 공정이 한계에 다다랐다고 진단하고 있다.



〈자료〉 위키피디아

[그림 1] 무어의 법칙: 집적회로 칩상의 트랜지스터 수(1971~2016년)

1) 무어의 법칙: 반도체 집적회로 성능은 18개월마다 2배씩 증가한다

한정된 면적에 트랜지스터를 보다 많이 집적하기 위해 노력한 결과, 트랜지스터 크기는 원자 수준으로 작아졌으나 양자역학에서 말하는 터널링 현상이 발생하여 회로를 구성하는 원자의 전자가 다른 곳으로 워프하는 현상이 생겨 근접회로에 합선이 발생하는 등의 전류 제어 문제가 제기되고 있다. 이러한 문제로 인해 인텔은 2016년 이후 공정주기를 2년에서 3년으로 전환한다고 발표하였고 "Cannon Lake" 프로세서는 10nm 공정이[2] 적용되어 2017년 출시할 예정이었으나 여러 차례 보류된 후 2018년 모바일 플랫폼에서 작동하는 i3-8121U 1기종만이 시험작으로 겨우 출시된 상황이며, 그 대안으로서 인텔은 Cannon Lake의 선행 모델로 10nm 공정이 처음으로 적용된 "Ice Lake"를 2019년 8월에 11종 출시하였다[21]. 그러나 7nm 이하로 공정을 줄이는 것이 앞서 언급한 터널링 현상 등으로 인해 어려울 것이라는 대다수 전문가들의 예상을 깨고 AMD는 CES 2019에서 7nm 공정에서 생산된 3세대 라이젠 프로세서 '마티스'와 라데온 VII 그래픽칩셋을 보란 듯이 발표하였으며, 라이젠 프로세서 시제품은 인텔 9세대 최상위 코어(i9-9900K)와 유사한 성능을 갖는다고 발표하였다[23].

한편, 삼성전자는 EUV(극자외선) 기술을 기반으로 "5나노 초미세 공정" 개발에 성공하였다고 2019년 4월 발표하였으며[12], 4월 중으로 7나노 제품을 출하하고 2019년 중 6나노 제품 설계를 완료하고 양산한다는 목표 아래 초미세 공정에서 선도적 역할을 수행하고 있다. 나아가 3nm GAA(Gate-All-Around) 공정 개발도 현재 진행 중이라고 보고하고 있는데, 앞으로도 당분간 초미세공정 개발 추세는 지속화될 전망이다.

현재까지 무어의 법칙을 이끌어왔던 공정 세밀화 및 실리콘 기반 반도체의 한계를 극복하기 위한 대안으로는,

- 산화갈륨(Ga_2O_3)이나 그래핀/탄소나노섬유를 재료로 하는 탄소 기반 반도체 등 신소재의 활용을 시험하는 방안,
- 한정된 칩 공간을 보다 효율적으로 활용하기 위해 여러 층으로 쌓아 올리는 적층 방식으로서의 3차원 적층,
- 광자를 이용한 광학 회로 활용 방법 등이 활발히 연구되고 있다.

그러나 이와 같은 기술적인 문제 외에도 반도체 집적화는 경제적인 측면에서 새로운 문제에 직면해 있다. 과거에는 집적도가 증가함에 따라 원가절감도 동시에 이루어졌으나

2) 10nm 공정: 기존 14nm 공정보다 2.7배의 트랜지스터를 더 집적할 수 있음

칩의 회로선폭이 28nm보다 줄어든 공정 이후부터는 디자인 및 제작비용이 급상승하는 현상이 발생하고 있다. 주된 이유는 새로운 공정인 실리콘 와이퍼를 새로 가공하는 공정이 추가된 것을 들 수 있으며, 과거 10년 전 65nm 집적회로를 개발하는데 1,600만 달러가 소요되었다면 14nm의 칩 개발에는 1억 3,200만 달러로 거의 10배 이상 비용이 치솟아 이러한 손실을 만회하기 위해서는 개발 비용의 7.5배인 9억 8,700만 달러의 수익을 올려야 하는 부담이 존재한다는 데 문제의 심각성이 있다[22]. 따라서 양자 컴퓨터는 이와 같은 초미세 공정이 한계에 다다르고 이를 통해 더 이상 추가적인 경제성을 기대할 수 없는 단계에 도달할 때 활용할 수 있는 대안으로서 검토되고 있다.

나. 에너지 효율 측면의 이슈

주요 선진국을 중심으로 현재 운영 중인 슈퍼컴퓨터의 대규모 전력 소모가 큰 문제점으로 부각되고 있다. 예를 들면, 중국 슈퍼컴퓨터 'Tianhe-2'의 소비 전력량은 24MWh로 이는 중소 도시 전체 공급 수준의 전력 소모에 해당하며, 일본을 대표하는 슈퍼컴퓨터 '京(케이)'의 경우 연간 전력 소비량은 9.89MWh로 연간 에너지 비용도 1,000만 달러에 달한다. [표 2]는 국내 KISTI 슈퍼컴퓨터와 관련한 2017년 1월부터 2019년 5월 말까지의 월평균 전력소모량과 전기료, 연간 전력 효율지수(Power Usage Effectiveness: PUE)를[3] 보여주고 있다. 참고로 2017년에는 슈퍼컴퓨터 4호기만 운영되었고 2018년은 4호기의 서비스와 5호기의 안정화 테스트가 진행되던 시기이며, 2019년은 슈퍼컴퓨터 5호기만 운영 중인 1월부터 5월 말까지의 자료 평균이다. 5호기 도입에 따른 절감 효과는 연간 데이터가 집계되어야 알 수 있겠지만, 2019년 5호기 운영 결과 PUE가 과거에 비해 개선

[표 2] KISTI 슈퍼컴퓨터 월평균 전력 소모량 및 전기료 현황(2017~2019년)

구분	평균 전력 소모량	월평균 전기료	연간 전력 효율지수
2017년	1,805,564kWh	1억 7,855만 원	1.56
2018년	3,567,763kWh	3억 6,404만 원	1.59
2019년(1~5월 말)	2,627,566kWh	3억 4,438만 원	1.36

〈자료〉 KISTI 내부자료

3) PUE(Power Usage Effectiveness)는 데이터센터의 에너지 효율을 나타내는 지표로서, 데이터센터 총 전력 사용량을 IT 장비의 전력소비량으로 나눈 값으로 일반적인 데이터센터의 PUE는 약 2.0이며 첨단 데이터센터의 경우는 1.38정도이다. PUE를 사용함으로써 전력사용량에 대한 정확한 정보를 파악하여 전력사용 통계, 재무나 회계 등에 활용할 수 있다(네이버 지식백과, IT용어사전에서 인용).

되었음을 알 수 있다.

최근 들어, 인공지능 기술을 이용하여 데이터센터의 에너지 소모를 줄이고자 하는 시도가 잇달아 소개되었는데, 구글의 경우 딥마인드(DeepMind) 신경망과 머신러닝을 활용하여 데이터센터 냉각 전력의 40%(PUE 15%에 해당)를 감소했다고 보고한 바 있다[18].

KT는 자체 개발한 인공지능 솔루션인 'e브레인'과 이를 바탕으로 구축된 "에너지 관리 시스템(Micro Energy Grid: MEG)"을 활용하여 개별 빌딩 및 사업장 등의 전력사용 데이터나 설비 작동 상황, 빅데이터 등을 분석함으로써 에너지 사용의 효율을 기하고 있다. KT는 에너지관제센터를 2015년 오픈한 후 협력기관(공단, 병원 등)에 에너지관리시스템을 설치하여 에너지 비용 절감에 노력한 결과, 목포에 위치한 한 병원에서 에너지 관제센터의 도움을 받아 연간 3억 원대의 에너지 비용을 9,000만 원으로 줄임으로써, 70%의 연간 비용절감이 발생했다고 보고한 바 있다[19]. 이처럼 AI 기술을 이용하여 에너지 비용 절감을 이룬 사례가 언론을 통해 공개되고 있으나, 에너지 비용을 획기적으로 감소시키는 데는 어느 정도 한계가 존재한다. 참고적으로, 양자컴퓨터의 경우 월평균 전력 소모량은 1,000~2,000kWh 정도가 필요할 것으로 전망되어 기존 슈퍼컴퓨터 전력 소모량과 비교해볼 때 에너지 소비를 획기적으로 감소시킬 것으로 예상된다.

2. 양자컴퓨터 기술개발 현황

기존 컴퓨터와 비교해 볼 때, 양자컴퓨터는 [표 3]과 같은 특성[16]을 지닌다.

[표 3] 기존 컴퓨팅 vs. 양자컴퓨팅

구분	주요 내용
통신능력 측면	분산컴퓨팅 환경에서의 고전적 통신 방식에 따르면, 물리적으로 분리된 노드 간의 상호 정보를 전달하기 위해서는 정보 자체를 전송하는 방법이 유일하다. 반면에 양자정보에서는 선제적으로 얽힘을 공유할 때 양자정보를 손쉽게 전송 및 상호 공유할 수 있을 뿐만 아니라 이를 통해 통신복잡도를 현저하게 낮출 수 있다는 장점을 지닌다.
계산능력 측면	양자컴퓨터는 양자정보의 중첩, 간섭, 얽힘 특성을 이용하여 처리하고자 하는 데이터 값들에 존재하는 전역적 특성을 쉽게 확인할 수 있어 복잡한 병렬 연산을 많이 요구하는 문제에서 특히 뛰어난 성능을 보일 수 있다.
보안능력 측면	양자정보의 관측붕괴성, 복제불가능성, 표현방식에서의 임의성 특성은 정보보호에서 기존 방식에 비해 보다 다양한 활용이 가능하다.

〈자료〉 최병수, "양자컴퓨팅시스템 개발 및 활용 동향", 2016.

이와 같은 양자컴퓨터의 특성을 구현하기 위해 디빈센조(DiVincenzo)는 양자컴퓨터가 기본적으로 충족시켜야 할 기술적 요구사항을 다음과 같이 제시하였다[2].

첫째, 양자상태를 잘 표현할 수 있는 큐비트를 구현할 수 있어야 한다. 소자 기술별로 큐비트를 정의하는 방식은 서로 상이하며, 이에 따라 구현방식이 다르므로 이러한 일련의 작업은 정보소자 의존적이다.

둘째, 큐비트의 상태를 초기화할 수 있어야 한다. 컴퓨터를 실행하는 과정에서 초기 상태의 확정은 매우 중요하다.

셋째, 연산이 수행되는 동안 충분히 긴 시간동안 양자결집상태(quantum-coherent state)를 유지할 수 있어야 한다. 다시 말해, 큐비트가 서로 결집되어 얽혀있는 상태를 일정 시간동안 충분히 유지시킬 수 있어야 한다.

넷째, 다양한 큐비트의 중첩상태를 변화시키는 메커니즘으로 양자 게이트(quantum gate)가 구현될 수 있어야 한다.

마지막으로 특정 상태에 따른 큐비트의 관측이 가능해야 한다. 계산의 중간 과정이나 최종 연산 결과를 도출하는 과정에서 해당 큐비트들의 관측이 가능해야 한다.

이와 같은 요구사항을 반영하여 양자컴퓨터를 구현하고자 할 때, 양자컴퓨터는 양자현상에 기반한 다양한 요소 기술이 융합되어 개발되는 종합기술이라고 할 수 있으며, 이를 구성하는 기술은 큐비트 생성, 얽힘 상태 유지, 양자 게이트 제어, 오류정정, 양자알고리즘 등의 분야[17]로 나누어 볼 수 있다.

현재 양자컴퓨터를 구성하는 핵심 요소 기술로서, 큐비트에는 초전도체 터널, 이온트랩, 반도체 양자점(스핀트로닉스), 광자 등 다양한 방식의 큐비트가 개발되고 있다. 다음의 [표 4]는 큐비트 소자 종류별 특성과 장단점을 보여주고 있다[11],[16].

이들 가운데 광자, 토폴로지, NV-Diamond 소자는 아직 기초 연구단계라 활용에는 많은 제약이 있는 상황이므로 현재 가장 많이 연구되고 있는 초전도 소자, 이온 트랩, 반도체 양자점(스핀트로닉스) 방식을 중심으로 좀 더 살펴보면 다음과 같다[17].

초전도체 방식은 절대온도 0℃ 부근에서 저항이 사라지는 초전도 현상을 이용하는데 이때 조셉슨 접합이라는 전자소자를 이용한다. 조셉슨 접합은 두 개의 초전도체 사이에 얇은 절연체를 끼운 소자로, 원래 절연체 때문에 전류가 흐르지 않아야 하지만 양자역학적 터널링 효과로 인해 초전도체에서 전류가 흐르게 되고 이 때 전류는 두 개의 전자가 쌍을

이루는 쿠퍼쌍(Cooper Pair) 형태가 되고, 이 쿠퍼쌍이 양자정보를 유지, 전달하며, 이 정보를 마이크로파로 조작하여 큐비트로 활용할 수 있다. 구글, IBM, D-Wave 등 양자컴퓨터 개발 경쟁에서 가장 앞선 그룹의 큐비트가 이와 같은 초전도 소자를 채택하고 있고 현재로서는 기술적으로 가장 앞선 상태이다.

[표 4] 큐비트 소자 종류별 특성

구분	특성	장단점	연구기관
초전도소자	초전도 전류의 공진 회로에 마이크로파를 인가해 전류의 양자중첩상태를 생성 큐비트 수: 16 연산 가능 수: 900 연산정확도: 99% 결맞음시간: 100μs 연산시간: ~0.1μs	[장점] 빠른 속도, 반도체 기술 활용 가능 [단점] 상태붕괴가 빠름. 초저온 유지	Google, IBM, Rigetti, Quantum Circuits
이온트랩	이온화된 원자의 최외각 전자의 에너지를 양자상태로 하고 레이저 쿨링과 포획을 통해 중첩상태 형성 큐비트 수: 5 연산 가능 수: 500.000 연산정확도: 99.9% 결맞음시간: 50μs 연산시간: ~10μs	[장점] 소자의 안정성, 높은 게이트 신뢰도 [단점] 속도가 느리고 다수의 레이저 장치가 필요함	IonQ
반도체 양자점 (스핀트로닉스)	반도체 양자점에 전자를 주입해 인공원자를 만들고 마이크로파로 전자의 양자상태를 제어 큐비트 수: 2 연산 가능 수: 120 연산정확도: 90% 결맞음시간: 120μs 연산시간: ~1μs	[장점] 소자의 안정성, 반도체 기술 활용 가능 [단점] 얽힘상태 구현이 어렵고 초저온 유지	Intel
광자	큐비트로 얽힘 상태의 광자를 생성하는 방법으로는 자발매개하향변환(SPDC)과정이 가장 널리 이용되고 있음	[장점] 양자컴퓨터뿐만 아니라 양자통신, 양자센서 등 다양한 영역으로 확장 가능 [단점] 광속으로 움직이는 광자의 운동성과 휘발성으로 집적소자 개발이 어려움	Purdue University, MIT
토폴로지	반도체 채널을 따라 흐르는 전자특성 중에 나타나는 가상입자를 이용	[장점] 에러가 발생하지 않음 [단점] 구현 가능성 입증되지 않음	Microsoft
NV-Diamond	다이아몬드 구조안의 질소와 동공의 스핀상태를 레이저로 제어	[장점] 상온 작동 [단점] 얽힘상태 구현이 어려움	Quantum Diamond Technologies

주) 자발매개하향변환(Spontaneous Parametric Down-Conversion: SPDC) 과정이란 하나의 펌프 광자가 비선형 결정을 지나면서 일정 확률로 두 개의 "낮춤-변환된 광자"로 변환되는 과정으로, 에너지와 운동량 보존이 모두 만족되는 조건하에서 일어나고 이렇게 생성된 광자는 결맞음 특성 및 양자얽힘 등의 양자역학적 특성을 지니고 있기 때문에 광학소자들을 이용한 추가적인 조작을 통해서 원하는 양자상태로 변환할 수 있음[14]

〈자료〉 과학기술정보통신부, 양자컴퓨팅 중장기 추진전략 기획연구, 2018./ETRI, "양자컴퓨터 기술 연구개발 동향", 2018. 2.

이온 트랩은 전자기장을 이용하여 전하를 갖는 입자를 3차원 공간에 가두는 장치로서, 원하는 만큼 정확한 개수의 이온을 장시간 유지할 수 있어서 양자컴퓨터 및 양자암호통신 개발이 활발히 진행되고 있다[10]. 양자역학 실험의 특성상 중첩된 양자상태는 측정 시 붕괴되어 버리는 속성으로 말미암아 매번 반복 실험을 거쳐야만 하는데, 다른 여타의 기술과 비교하여 이온 트랩 기술은 포획된 입자를 비교적 장시간 유지할 수 있다는 장점 때문에 동일 입자를 통한 반복 실험이 가능하다는 장점을 갖는다. 또한, 진공 중의 전기장을 이용하여 이온을 포획한다는 장점으로 말미암아 주변 환경으로부터의 간섭이 거의 없다는 장점도 지닌다.

반도체 양자점(스핀트로닉스) 방식의 장점은 기존 반도체 소자를 큐비트로 이용하는 방식으로 반도체 집적기술을 그대로 이용할 수 있을 뿐만 아니라, 다른 방식에 비해 양자의 스핀제어가 쉽고 집적화가 쉬우며 양자정보를 조작하는 속도 또한 빠른 반면, 조작 가능한 양자의 수는 2큐비트에 불과해 앞서 소개한 초전도 방식이나 이온트랩 방식보다는 못하다는 단점을 지닌다.

그러나 어떠한 큐비트 기술이 적용되더라도 대규모 양자컴퓨터를 위해서는 많은 수의 큐비트에 대해 많은 연산이 가능해야 하고 정확도와 신뢰성 또한 높아야 한다. 이러한 맥락에서 현재 많은 큐비트 관련 소자 기술은 큐비트 수를 늘리는 연구에 집중함과 동시에 조작과정에서의 오류를 낮추는 방향으로 연구가 진행되고 있다[11],[16].

III. 국가별 양자컴퓨터 관련 주요 R&D 정책 및 현황

1. 국가별 양자컴퓨터 R&D 정책

미국을 비롯한 세계 주요 국가들은 양자컴퓨터 분야의 주도권을 확보하고자 양자컴퓨터 개발에 특화된 정책을 경쟁적으로 수립하고 막대한 예산을 투자하고 있다. 특히, 양자컴퓨터, AI 등의 첨단 기술 연구 개발에 있어서 중국의 약진은 미국이 세계 시장에서 기술의 리더십을 점차 잃어가는 것이 아닌가하는 우려를 자국 내에 불러 일으키고 있다.

가. 미국

미국 트럼프 대통령은 2018년 12월 양자컴퓨팅 분야 R&D 전략투자 정책방안 제시를

위해 국가 양자 이니셔티브(National Quantum Initiative: NQI) 법안에 서명하였고 이에 따라 백악관 과학기술정책실(OSTP) 내에 국가양자조정실을 설치하여 기술 지원 및 홍보에 대한 주도적 역할을 부여하여 향후 5년간 연간 2,500만 달러를 집행할 계획이다.[4] 부처별로는 국방부(DoD), 표준기술연구소(NIST), 국립과학재단(NSF), 민군겸용 기술개발청(DARPA), 고등정보기술개발청(IARPA), 미국항공우주국(NASA), 전미과학아카데미(NAS) 등의 정부기관은 물론 민간 연구소(IBM, HP, BELL), 대학(MIT, Stanford, Caltech) 등에서 후속 연계 기술을 지속적으로 개발하고 있다[6]-[8]. [표 5]는 국가 양자 이니셔티브 법에 다른 신설 정책을, [표 6]은 국립과학재단(NSF)의 양자과학 지원 프로그램의 사례를 보여주고 있다.

[표 5] 국가 양자 이니셔티브 법에 따른 신설 정책

정책	주요 역할
국가 양자 이니셔티브	- 국가 양자 과학에 대한 목표와 과제, 성과 척도를 설정 - 양자정보과학 R&D에 대한 투자 - 국가 양자 조정실 설치
양자정보과학소위원회	- 연방기관의 양자 관련 정책 조율, 국가 양자 이니셔티브 목표 설정, 국내 및 국외의 양자 과학 R&D 현황 파악 - 양자 정보 과학 R&D 예산 신청
국가 양자 이니셔티브 자문위원회	- 양자정보과학 R&D, 표준, 교육, 기술이전, 상업화, 국방, 경제 등과 관련한 자문과 정보 제공 - 정기적으로 대통령과 의회에 관련 보고서 제출

〈자료〉 KISTEP, "과학기술&ICT 정책·기술동향", 2019. 3.15.

[표 6] 국립과학재단(NSF)의 양자과학 지원 프로그램

연구 분야	주요 내용
양자통신	- 2016년 8월, 국립과학재단은 보안성이 뛰어난 양자통신 기술의 발전을 위해 1,200만 달러를 투자
양자컴퓨터	- 2018년 8월, 국립과학재단은 사상 최초의 실용적 양자컴퓨터를 만드는데 1,500만 달러를 투자
차세대 인력 양성	- 대학의 책임연구자, 기업 파트너, 대학원생으로 구성되는 양자 정보과학공학 네트워크(QISE-NET)를 3년 간 지원

〈자료〉 KISTEP, "과학기술&ICT 정책·기술동향", 2019. 3. 15.

나. 영국

영국 정부는 양자정보과학의 발전을 위해 2014년 국가 양자기술 프로그램(UK National Quantum Technologies Programme)을 출범하였고 출범 이후 현재까지 누적 투자액

4) 2018년 9월 국가과학기술위원회(NSTC)가 발표한 '양자정보과학 국가전략'을 바탕으로 수립

이 10억 파운드(약 12억 7,000만 달러)를 넘어서고 있다. 이 프로그램은 통합 컨트롤 타워로 양자기술전략위원회(Quantum Technologies Strategic Advisory Board: QTSAB)가 주관하고 있으며, 각 정부부처 및 산하 연구기관이 참여하고 있다. 참여 기관들은 프로그램의 집행을 모니터링하고 필요시 기관 단위에서 추가적인 예산지원까지 수행한다. 특히, 2015년에는 향후 20년간의 국가 연구개발 전략과 양자기술 로드맵이 작성되어 발표되었다. 양자기술 로드맵에서는 단기, 중기, 장기 기간별 상용화 가능 기술과 각 기술의 예상 시장규모가 전망되어 산업계의 혁신과 참여를 유도하고 있다. 또한, 2019년 6월에는 양자컴퓨팅 상용화 및 사업화 지원에 1억 5,300만 파운드 (약 1억 9,400만 달러)를 투자한다고 발표하였다[20].

초기 단계의 양자 분야 스타트업 기업 지원을 위해 조성된 기금 1억 5,300만 파운드는 벤처 기업의 설립과 야심찬 사업화 계획에 대한 지원뿐만 아니라, 관련 분야 간의 협업 R&D 프로젝트와 혁신적인 아이디어에도 투자될 예정이다. 영국의 이러한 투자확대 정책은 영국의 브렉시트(Brexit) 선언 후 유럽과의 단절을 우려한 조치라고 보여진다. 유럽연합(EU)에서는 2016년부터 “Quantum Manifesto” 프로젝트를[5] 진행하여 오고 있다.

다. 중국

중국은 추진해야 할 중점 연구 분야 중 하나로 양자컴퓨터를 선정하고 양자통신, 양자컴퓨터 산업 육성을 골자로 하는 로드맵을 영국과 마찬가지로 2015년에 발표하였다. 그러나 미국, 영국 등 서구 선진국이 국가의 직접적인 개입보다는 대학과 민간기업 위주로 기초연구를 수행하고 있는데 반하여, 중국은 국가 주도의 중장기 연구개발 계획 아래, 세부 연구 분야별로 상세한 개발 로드맵을 설정하고 지속적인 연구개발자금을 투입하고 있어, 비교적 단기간에 기술축적이 상당한 수준으로 이루어져 왔고 특히 양자암호통신 분야에서는 이미 미국을 추월한 것으로 평가되고 있다.

중국의 양자정보과학 분야 주요 연구개발 계획을 살펴보면 [표 7]과 같다[17]. 중국에서도 양자컴퓨팅 분야는 민간 영역의 비중이 커지고 있는 추세이며, 2015년 알리바바(Alibaba)와 공동 출범한 양자컴퓨터 연구소를 통해 2025년까지 현재의 슈퍼컴퓨터에 필적하는 계산속도를 가지는 양자 시뮬레이터를 개발하고 2030년에는 500~1,000 큐비

5) “Quantum Manifesto” 프로젝트: 2018년부터 10년간 4대 분야(양자통신, 양자소자·계측, 양자컴퓨터, 양자시뮬레이션)에 10억 유로(약 1조 3,300억 원) 투자

[표 7] 중국의 양자정보과학 분야 연구개발 계획

계획명(기간)	주요 내용
제13차 중국 5년계획 (2016~2020)	- 국가의 전략적 연구개발 항목 중 하나로 “Quantum Control”을 지정하여 양자정보과학에 대한 전략적 접근을 제시
국가중점연구계획 (2016. 2)	- 최우선 연구과제로 Quantum Control과 양자정보를 포함시키고 후속 가이드라인에서는 6개 세부항목을 지정
제13차 중국과기혁신계획 (2016.8)	- Quantum Control과 양자정보를 최고 전략목표로 선정하여 국제 기술 경쟁에서 확고한 우위를 점유하는 것을 국가 전략으로 천명 - 2030년 국가 전략과제 목표로 대도심 및 도시간 자유공간(free space) 양자통신기술, 범용 양자컴퓨터 프로토타입, 양자 시뮬레이션 개발과 양자항법을 이용하는 항공 및 우주개발을 선정
중국 제조 2025 (2015)	- 제조업의 경쟁력 향상을 위한 상용기술 확보 목표 중 하나로 양자 컴퓨터를 차세대 정보통신 기술산업 중 하나로 선정

〈자료〉 KISTI, “양자컴퓨팅 연구개발 동향 연구”, 2018. 12.

트의 범용 양자컴퓨터를 개발한다는 계획을 갖고 있다. 또한, 2018년부터 5년간 1,000억 위안(약 17조 원)을 투입하여 안후이성에 양자정보과학 국가연구소 설립을 추진하고 있는데, 원거리 양자통신망 구축과 양자컴퓨터 개발을 목표로 하고 있다.

라. 일본

일본은 세계 최초로 NEC에서 초전도 스핀 큐비트 개발에 성공하였고 양자 어닐링 이론 제안 등 양자컴퓨팅 분야에 있어서 핵심 이론과 주요 요소기술의 개발을 선도해 오고 있으며, 일본 정부 또한 2008년부터 꾸준히 양자컴퓨팅 분야를 정책적으로 지원하여 오고 있다. 예를 들면, 2009년부터 2013년까지 추진된 최첨단 연구지원 프로그램(FIRST)에서 “양자정보처리 프로젝트”를 수행하면서 세부과제로 일본 독자적인 레이저 네트워크 방식의 양자컴퓨터를 개발하였으며, 후속 연계 프로그램으로 2014년부터 시작된 혁신적 연구개발 추진 프로그램(ImPACT)에서는 “양자 인공두뇌를 양자 네트워크로 연결한 고도 지식사회 기반 실현”을 목표로 양자 인공지능 개발을 진행 중에 있다. 본 연구를 위해 5년간 30억 엔이 투자되었다[13][15].

2016년에 발표된 “제5기 과학기술 기본계획”에 따르면, “광·양자 기술”을 새로운 가치 창출의 핵심 기반 기술로 지정하였고 이에 따라 2016년 3월부터 “과학 기술·학술심의회-첨단연구기반부/양자과학기술위원회”에서 양자과학 기술의 추진 방안에 대한 조사 검토에 착수하였다. 같은 시기에 문부과학성은 JST 전략적 창조 연구추진사업(신기술 창출)의 2016년 전략 목표의 하나로 “양자 상태의 고급 제어에 의한 새로운 물성 정보 과학 프론

티어의 개척"을 결정하였고 4월부터 JST에서 전략목표에 따른 기초 연구 지원을 시작하였다. 최근의 문부과학성 사례로는 슈퍼컴퓨터를 능가하는 양자컴퓨터를 실용화한다는 방침 아래 2018년부터 "Q-LEAP 프로그램(광·양자 도약 플래그십 프로그램)"을[6] 추진하고 있다.

2. 양자컴퓨터 개발을 둘러싼 주요 선행 기업 동향

양자컴퓨터 개발은 IBM, Google, Microsoft, Intel 등 미국의 거대 IT 기업들이 기술 개발을 주도하는 가운데 일본, 중국, 유럽의 주요 기업들도 참여하여 각축전을 벌이고 있다. 이들 기업 중 IBM은 양자 컴퓨터 기술 개발에서 "Quantum Supremacy(양자컴퓨터가 기존 컴퓨터를 능가하는 성능을 입증하는 것)" 자리를 놓고 구글과 경쟁하고 있는 양자컴퓨터 분야에서 가장 앞선 기업 중의 하나로 1997년 아이작 추앙이 2비트 양자컴퓨터를 최초로 개발한 이래, 처리 큐비트 수를 늘린 양자 프로세서를 지속적으로 공개하고 있다. 2017년 12월에는 세계 12개 기관과 공동연구 계획을 발표하여[7] 진행하고 있으며, 양자컴퓨팅 개발 이니셔티브를 "IBM Q"라고 명명하고 공동연구 대학들[8] 내부에 기술개발 허브를 설립하였다.

구글(Google)은 2009년에 D-Wave 시스템 도입으로 양자컴퓨터 연구를 시작한 이래, 2014년 UCSB(University of California, Santa Barbara)의 존 마티니스(John Martinis)[9] 박사 영입을 통해 차별화된 연구 개발을 본격적으로 시작하였다. 존 마티니스 박사의 주도 아래 구글은 양자컴퓨터 분야의 후발주자에서 탈피하여 여러 앞선 경쟁자를 따라잡는 분기점을 마련하였고 2018년 3월에는 IBM의 50 큐비트를 넘어서는 72 큐비트의 양자 프로세서를[10] 공개하였다. 구글의 양자컴퓨터 개발 방식은 아날로그 방식에 독자적으로 개발한 디지털 기술을 통합한 하이브리드 방식이란 점이 특징이고 이를 통해 아날로그 방식인 단열 양자컴퓨터 기술을 디지털 방식으로 보완하였다. 구글의 양자 컴퓨터는 자사 클라

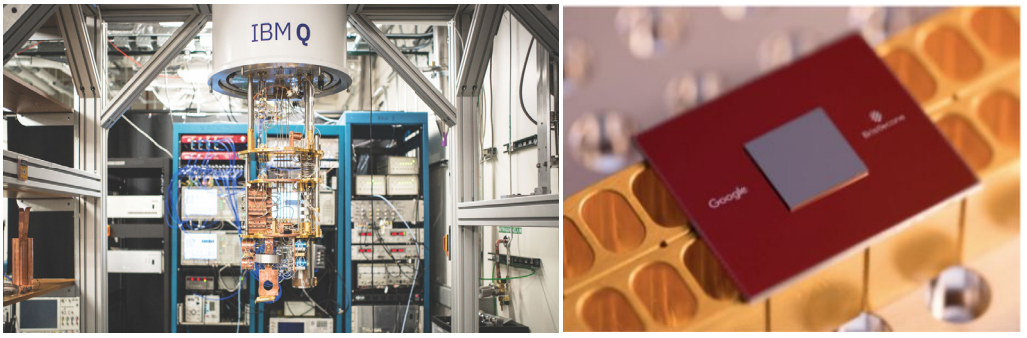
6) 2018년부터 10년간 약 300억 엔(한화 약 3,069억 원)을 투입할 예정이며, 2018년 예산은 22억 엔

7) IBM은 8개 글로벌 기업 및 4개 대학/연구소 등 12곳과 협업하여 20 큐비트 양자컴퓨터 기술 개발에 나선다고 발표하였고 동 연구에 삼성전자와 자동차 제조업체 Honda, Daimler가 참가. 파트너로 JP Morgan Chase, Barclays 은행, 일본의 고분자 화학기업 JSR, 화학상사 Nagase, 원자재 회사 Hitachi Metals 등이 참가. IBM은 참가 파트너에 양자컴퓨팅 초기 접근 프로그램인 Q Network를 제공

8) 공동연구 대학/연구소로 선정된 곳은 미국 에너지부 산하 오크리지국립연구소, 영국 옥스퍼드대학, 호주 멜버른대학, 일본 게이오대학 등

9) John Martinis 박사는 UCSB 교수이자 1980년대부터 양자를 연구해온 물리학자로 2014년 교수직을 유지한 채 Google에 합류해 양자컴퓨터 개발을 주도

10) 양자게이트 방식 중 지금까지 발표된 최고 큐비트의 양자 프로세서임



〈자료〉 IBM의 IBM Q 양자컴퓨터/구글, “양자컴퓨터 개발 새장... 72큐빗 칩 선보여”, 2018. 12. 23.

[그림 2] IBM Q 양자컴퓨터와 구글에서 개발한 72큐비트 프로세서

우드 플랫폼을 통해 제공될 예정이며, 이는 양자컴퓨터를 AI 다음의 핵심기술로 인식하고 클라우드를 통해 제공하겠다는 IBM 전략과 유사하다. 구글이 자사의 클라우드 플랫폼을 통해 양자컴퓨팅 자원을 제공하는 또 다른 목적은 양자컴퓨터를 위한 알고리즘 및 응용 프로그램 개발을 촉진하겠다는 의도로 볼 수 있으며, 구글은 하이브리드 방식의 양자컴퓨터 활용 연구자를 늘리고 개발자 커뮤니티를 형성하고자 하는 목표를 갖고 있다.

마이크로소프트(Microsoft: MS)는 양자컴퓨터가 곧 미래라는 인식 아래 하드웨어 외에도 소프트웨어 개발에 주력하고 있다. 먼저 하드웨어 개발과 관련해서는 2005년 세계적인 수학자 마이클 프리드먼(Michael H. Freedman)을 영입, 양자 컴퓨터 개발을 위한 전문 연구소 “Station Q”를 설립하여 범용 양자컴퓨터 개발을 본격화하였다. 개발 방식은 “위상 양자컴퓨터(Topological Quantum Computer)”인데 오류에 대한 내성이 높은 구조를 특징으로 하지만 매우 어렵고 아직 초기 단계라 장기적인 연구가 소요된다는 점이 단점이다. 특히, 사용 소자인 마요라나 페르미온(Majorana Fermion)은 2012년 네덜란드 Delf 대학 연구진이 처음 관측에 성공하였으나 아직 완전히 해명되지 못한 상태이다[15].

마이크로소프트는 양자 소프트웨어 개발에도 주력하고 있는데 2011년 양자컴퓨터 소프트웨어 개발 부문인 “Quantum Architectures and Computation Group(QuArC)”를 개설하였다. QuArC의 주요 목표는 양자 컴퓨터 개발과는 별도로 사회에 도움이 되는 양자 응용 프로그램을 개발하고자 하는 것이다. 2017년 9월에는 미국 플로리다주 올랜드에서 개최된 연례행사(Ignite Conference)에서 개발자 전용 위상 큐비트(Topological Qubit)와 운영시스템을 공개하였으며, 이어 2017년 12월에는 양자컴퓨터 특화 언어인

‘큐삽(Q#)’이 포함된 퀀텀 개발 키트 베타를 공개하였다. 큐샵은 MS의 장점인 전통적인 프로그래밍 개념을 양자컴퓨팅 분야에 도입할 목적으로 개발된 것이다. 업계에서는 기존 소프트웨어 시장을 석권했던 MS가 승리 방정식을 양자컴퓨터 시장에서도 재현하려는 시도라고 분석하고 있다.

인텔(Intel)은 실리콘 기반의 양자컴퓨터 개발에 집중하고 있으나 자체 개발 내용은 잘 알려져 있지 않은 가운데 2015년 네덜란드 TU Delft/TNO 대학의 양자연구소 QuTech에 10년간 5,000만 달러를 투자하였고, 이를 통해 2017년 17 큐비트 양자 프로세서 공개를 시작으로 불과 3개월 뒤에는 CES 2018에서 49 큐비트 양자프로세서를 공개하는 등 매우 빠른 행보를 보이고 있다. 인텔은 자체 로드맵을 통해 향후 5~7년 이내에 1,000 큐비트 시스템 확보를 목표로 하고 있다.

마지막으로 소개할 D-Wave Systems는 캐나다에 기반을 두고 1999년에 설립된 벤처기업으로 양자컴퓨팅 개발을 표방한 최초의 양자컴퓨터 상용화 기업이다. 2007년 2월에 큐비트 양자컴퓨터 시연에 이어 2011년 5월에는 세계 최초로 128 큐비트의 상용 양자컴퓨터 “D-Wave 1”을 개발하여 양산을 시작하였으며 이를 통해 양자컴퓨터 상용화의 발판을 마련하였다. “D-Wave 1” 출시 당시에는 진정한 의미의 양자컴퓨터인가에 대한 논란이 있었으나, 구글과 NASA의 실험결과 특정 문제에 대해 1억 배 이상의 처리속도 향상이 있었음이 확인되었다. D-Wave Systems는 계속해서 신제품을 출시하였는데, 2013년 5월엔 512 큐비트의 “D-Wave 2”를 개발했고, 2015년 8월 1,000+ 큐비트의 “D-Wave 2X” 시스템을, 2017년 1월에는 2,000+ 큐비트의 “D-Wave 2000Q”를 개발하여 오고 있으며, 인텔, 히타치, 후지쓰에 뒤이어 2019년 7월 말 현재 118건의 양자컴퓨터 관련

〈자료〉 D-Wave Systems

[그림 3] D-Wave 양자컴퓨터

특허를 보유하고 있다.

현재 D-Wave Systems의 양자컴퓨터를 처음 도입한 Lockheed Martin 외에 Google, NASA, USC(University of Southern California) 등에서 다양한 잠재력 연구 및 실증 실험에 D-Wave 시스템을 활용하고 있다.

3. 양자컴퓨터 개발관련 국내 동향

과학기술정보통신부는 2019년 “양자컴퓨팅 핵심원천기술 확보[11] 및 국내 연구생태계 조성”[12] 사업을 통해 향후 5년간 양자컴퓨터 하드웨어 등 핵심원천기술 개발과 양자컴퓨팅 신(新)아키텍처, 양자알고리즘, 기반 소프트웨어 등 미래 유망 분야에 총 445억 원을 투자할 계획으로 2019년에는 총 60억 원이 투입될 예정이다[9].

국가과학기술지식정보서비스(National Science & Technology Information Service: NTIS)의 국가 R&D과제를 살펴보면, 그 이전에도 양자컴퓨터에 대한 연구는 국가 R&D 차원에서 수행되었음을 알 수 있다. 2002년부터 2017년까지의 통계를 살펴보면, ‘양자컴퓨터’ 또는 ‘양자컴퓨팅’이란 검색어로 총 265건의 과제가 도출되었다. 전체 투자 규모는 총 496억 원으로 연평균 33억 원이 투자되었는데 여기에는 NTIS에서 집계되지 않은 민간기업의 자체 개발비용 등은 포함되지 않았다. 그러나 지금까지의 연구는 과제단위의 실험적 성격의 과제가 많고 ‘양자컴퓨터’라는 명시적인 주제로 사업이 본격화되기 시작한 것은 2019년부터라고 볼 수 있다[17].

민간 기업 차원에서는 앞서 살펴보았듯이, IBM이 2017년에 시작한 양자컴퓨터 기술 공동개발 국제 협업연구에 삼성전자가 양자컴퓨팅이 반도체에 미치는 영향을 연구하기 위해 참여하고 있으며, SKT는 양자 소프트웨어 개발 스타트업으로 양자암호통신 1위 기업으로 평가받고 있는 IDQ를 2018년에 인수함으로써 관련 기술력을 성공적으로 확보하기도 하였다.

연구개발 차원에서는 한국과학기술원(KIST), 한국표준과학연구원(KRISS), 한국전자통신연구원(ETRI) 등 정부출연연구기관과 서울대, 한국과학기술원(KAIST), 고려대 등의 학계를 중심으로 양자컴퓨터 연구가 진행되고 있다. 큐비트 소자 종류별 연구기관 현황을

11) 2023년까지 5큐비트급 범용 양자 프로세서 구현→2027년까지 100큐비트 구현(후속사업) 등
12) 양자컴퓨팅 핵심원천기술 7팀, 미래유망기술 26팀 등 양자컴퓨팅 전문연구그룹 33개 이상 발굴 육성

살펴보면, 초전도 소자는 한국표준과학연구원, 건국대학교, 연세대학교, 한국과학기술원에서, 양자점 연구는 한국과학기술원, 한양대학교, 영남대학교에서, 스핀트로닉스 연구는 고려대학교, 영남대학교, 한국과학기술원에서, 광자에 관한 연구는 부산대학교, 포항공과대학교, 서울대학교에서 주도적으로 수행하고 있다[17]. NTIS 통계에 의하면, 대부분의 연구가 대학 63%, 출연연 32% 순이고 해외 공동연구 비중은 12%, 기업 공동연구의 비중은 9%로 아직 매우 저조한 것으로 나타났다.

Ⅳ. 결론 및 시사점

IBM, 구글 등 양자컴퓨터 분야의 주요 선도 기업들은 최근 클라우드를 통해 자사 양자컴퓨터 시스템에 접속하여 프로그래밍과 다양한 테스트를 진행할 수 있는 클라우드 기반 양자 서비스를 시작하거나 제공할 계획임을 밝히고 있다. 이는 양자컴퓨터에 대한 일반의 관심 확대는 물론 개발자 커뮤니티의 생성과 시장의 선점 및 확대까지를 고려한 전략적 행보로 예측된다. 아직 양자컴퓨터의 핵심이 되는 큐비트를 늘리는 경쟁과 계산과정에서 발생하는 오류를 정정하는 데 많은 연구가 집중되고 있기는 하지만, 이러한 가운데 선도 기업들이 양자컴퓨터에 기반한 클라우드 서비스를 서두르는 까닭은 결국 자사 양자컴퓨터에 특화된 알고리즘과 응용 프로그램 개발을 촉진시킴으로써 시장 선점으로 연계하는 한편, 자사 시스템 중심의 개발자 및 사용자 커뮤니티를 형성하고 강화시키려는 시도로 해석된다[13].

그러나 상대적으로 진입이 늦은 구글이나 인텔의 사례가 보여주듯이 양자컴퓨터 전문가의 영입, 집중적인 투자와 연구 개발을 통해 단기간 내에 얼마든지 선도 기업을 따라잡을 수 있음을 고려해보면, 여러 선도 기업의 약진에도 불구하고 양자컴퓨터 산업은 아직 태동기라고 진단할 수 있다. 따라서 정부는 더 늦기 전에 실효성 높은 양자컴퓨터 커뮤니티를 조성하여 장기 투자계획에 따른 연구개발 및 기술 특화 전략 마련 등 포괄적 양자컴퓨팅 육성을 위한 사업 계획 수립을 심도 있게 마련할 필요가 있다. 예를 들면, 미국, 중국과 같이 장기 로드맵을 작성하여 국가 주도적으로 기술을 육성하거나 영국의 사례와 같이 정부의 적극적인 지원을 통해 스타트업을 발굴하고 기술을 지원하는 국가 전략을 추진할 필요가 있다. 다만 제한된 예산 범위 내에서 모든 것을 다하려는 정책보다는 투자대비

실효성을 가져올 수 있고 주요 선도 기업이 아직 주목하지 않는 틈새 분야에 집중하는 전략이 보다 유효하리라 판단된다. 또한, 현재 대학과 연구기관들을 중심으로 산별적으로 추진되고 있는 사업을 체계적으로 결집시키는 노력을 시도할 필요도 있다고 본다. 예를 들면, 한국과학기술원이나 한국표준과학연구원에서 독자적으로 개발된 양자컴퓨터 자원을 한국과학기술정보연구원의 슈퍼컴퓨팅 자원과 밀결합하여 과학기술 분야 연구자에게 서비스하는 방안 등을 추진할 필요가 있다. 양자컴퓨터 기술 개발 못지않게 수요자 중심의 관련 생태계를 구축하려는 노력이 필요한 시점으로 보인다.

[참고문헌]

[1] David Deutsch, “Quantum theory, the Church-Turing principle and the universal quantum computer,” Proceedings of the Royal Society of London A 400, 1985, pp.97-117.

[2] David P. DiVincenzo, “The Physical Implementation of Quantum Computation,” Fortschritte der Physik, Vol.48, Issue 9-11, 2000. 9, pp.771-783.

[3] Minato, M., “量子コンピュータの最新動向”, GREE ventures, 2018.

[4] Peter Shor, “Algorithms for quantum computation: discrete logarithms and factoring,” SFCS ’94 Proceedings of the 35th Annual Symposium on Foundations of Computer Science, IEEE Computer Society Press, 1994, pp.124-134.

[5] Richard P. Feynman, “Simulating Physics with Computers,” International Journal of Theoretical Physics, Vol.21, Nos.6/7, 1982.

[6] 한국과학기술기획평가원(KISTEP), “과학기술&ICT 정책·기술동향”, Vol.114, 2018. 3. 16.

[7] 한국과학기술기획평가원(KISTEP), “과학기술&ICT 정책·기술동향“, Vol.138, 2019. 3. 15.

[8] 한국과학기술기획평가원(KISTEP), “과학기술&ICT 정책·기술동향“, Vol.148, 2019. 8. 2.

[9] 과학기술정보통신부, “꿈의 컴퓨팅, 양자컴퓨팅 핵심기술 개발 첫 발 뗀다”, 보도자료, 2019. 2. 1.

[10] 김태현, “이온트랩 시스템을 이용한 양자정보처리”, 한국광학회, 광학과 기술, Vol.18, Issue 2, 2014. 4, pp.26-31.

[11] 백충헌 외3, ”양자컴퓨팅 기술 연구개발 동향“, ETRI, 전자통신동향분석 33권 1호(통권 169), 4차 산업혁명 사회의 초연결 지능과 신뢰 인터넷 기술 특집, 2018. 2, pp.20-33.

[12] 삼성전자, “삼성전자, 최첨단 5나노 파운드리 공정 개발“, 보도자료, 2019. 4. 16.

[13] 이준 외1, “과학기술 한계 극복의 길을 여는 양자컴퓨터 : 양자컴퓨터 R&D 현황과 정책”, KISTI Issue Brief No.11, 2019. 7.

[14] 임향택 외4, “광자 기반의 양자정보 연구”, 한국광학회, 광학과 기술, Vol.18, Issue 2, 2014. 4, pp.6-12.

[15] 조성선, “양자컴퓨터 개발 동향과 시사점”, 정보통신기술진흥센터, ICT Spot Issue, S18-02, 2018. 2.

[16] 최병수, “양자컴퓨팅시스템 개발 및 활용 동향”, ETRI, 전자통신동향분석 31권 2호(통권 158),

2016. 4, pp.84-94.
[17] 한국과학기술정보연구원, “양자컴퓨터 연구개발 동향 연구”, 내부자료, 2018. 12.
[18] Chosun Biz, “블록체인AI뉴스”, 2018. 9. 26.
[19] Chosun Biz, [4차산업 생생현장]④인공지능으로 에너지 70%절약, KT 에너지관제센터를 가다, 2017. 1. 5
[20] Techcrunch, “UK government invests $194M to commercialize quantum computing,” 2019. 6. 13
[21] ITWorld, “인텔, 10세대 아이스레이크 칩 출시...노트북의 성능과 그래픽에 가져올 변화”, 2019. 8. 2.
[22] Chosun Biz, [무어의 법칙 폐기]①반도체 패러다임 대전환...IT융합 칩수요 다변화 시대, 2016. 4. 12.
[23] Zdnet, [CES 2019] AMD, 7nm 라이젠 프로세서 공개, 인텔 코어 i9-9900K 따라잡은 8코어 로세서 시연, 2019. 1. 10.

chapter 3

음성인식 성능향상을 위한 지능형 환경잡음감쇄 기술

정혜동 ‖ 전자부품연구원 책임연구원
김홍국 ‖ 광주과학기술원 교수

I. 결과물 개요

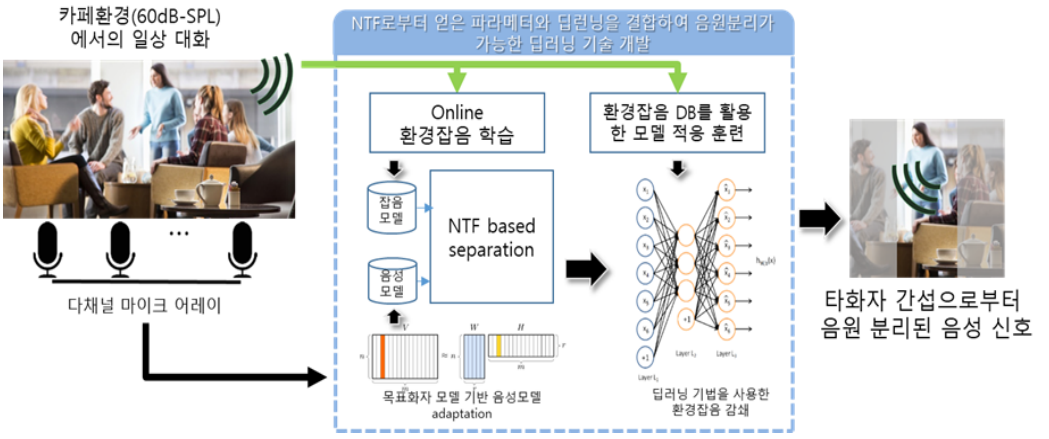
개발목표시기	2020. 12.	기술성숙도(TRL)	개발 후 TRL 6
결과물 형태	SW	검증방법	SNR 개선
Keywords	Noise reduction, Non-negative tensor factorization, Ideal ratio mask estimation		
외부기술요소	Tensorflow, armadilo, kiss FFT	권리성	SW/SW-IP

II. 기술의 개념 및 내용

1. 기술의 개념

➢ 최근 음성 개선(speech enhancement)의 경우 음성 기반의 애플리케이션의 발달과 함께 수요가 증가하는 추세에 있는데, 이는 많은 애플리케이션들이 잡음환경에서 음성

* 본 내용은 정혜동 책임연구원(☎ 031-739-7455)에게 문의하시기 바랍니다.
** 본 내용은 필자의 주관적인 의견이며 IITP의 공식적인 입장이 아님을 밝힙니다.
***정보통신기획평가원은 현재 개발 진행 및 완료 예정인 ICT R&D 성과 결과물을 과제 종료 이전에 공개하는 "ICT R&D 사업화를 위한 기술예고"를 2014년부터 실시하고 있는 바, 본 칼럼에서는 이를 통해 공개한 결과물의 기술이전, 사업화 등 기술 활용도 제고를 위해 매주 1~2건의 관련 기술을 소개함



[그림 1] 기술개념도

이 녹음되고 이러한 환경에서 녹음된 음원이 낮은 signal to ratio(SNR)에서 작동하는 경우가 있으며, 이에 따라 이러한 잡음 조건에서 잘 동작하기 위해 음성 개선은 음성을 활용하는 애플리케이션에 효과적으로 사용 가능하기 때문임

➢ 응용 서비스 환경에서 제공되는 다채널 마이크로폰 환경에서는 제공 환경마다 그 마이크 구조가 다양하여 적합한 전처리 기술이 필요함을 고려하여, 본 기술은 다채널 마이크로폰 환경에서의 전처리 기술의 하나로서 음성 잡음 분리를 목표로 함

2. 기술의 상세내용 및 사업화 제약사항

➢ 기술의 상세내용

- 제안 기술은 여러 배경 소음이 혼재하는 실제 환경에서 음성을 분리하는 방법에 있어서, 다채널 마이크 어레이를 활용한 비음수 텐서 분해 기법(Nonnegative Tensor Factorization: NTF)을 통해 실시간으로 동작함
- 특히, 외부 잡음들에 대해 잡음 모델을 실시간으로 적응 가능하며, 이를 통해 더욱 강건하게 잡음분리가 가능한 것이 특징임
- 또한, 본 기술은 딥러닝 기법을 활용한 스펙트럼 Ideal Ratio Mask(IRM) 추정 방법을 결합하여 더욱 강건한 잡음감쇄가 가능함

➢ 기술이전 범위

- 비음수 텐서 분해 기법 기반의 잡음감쇄 기술
- 비음수 텐서분해의 잡음모델 실시간 업데이트 기술
- 딥러닝 기반 스펙트럼 마스크 추정 기술

➢ 사업화 제약사항

- 응용 서비스에 따른 알고리즘 튜닝이 필요할 수 있음

III. 국내외 기술 동향 및 경쟁력

1. 국내 기술 동향

➢ 인공지능 관련 기술 동향

- 자율지능 디지털 동반자 기술을 위한 사용자 의도 및 맥락 인지 기술은 최근 2~3년간 다수의 기업에 의해 개발되고 있으나, 개발 기간이 짧은 것이 현실이며, 투입 인력이 부족할 뿐 아니라 서비스에 연계된 기술 개발 환경이 제대로 이루어져 있지 않아 개별적인 상황 인지 기술을 개발 중
- 음성, 텍스트, 영상, 스토리, 정형 및 비정형 데이터, 장치 정보, 공간 정보 등의 복합 인지 및 정보로부터 지식을 습득하고 사용자 상황을 파악하는 연구 및 개발은 개별 기관/기업이 해낼 수 없는 복합적인 기술로 시도하지 못한 단계임
- 근거리 음성인식을 위한 잡음에 대한 연구 개발은 수행되었으나, 로봇 등을 위한 원거리 음성인식 및 실제 잡음 환경에서의 연구는 초기 단계에 있으며, 원거리 음성인식을 위해서는 타채널 음질 개선 기술이 필수적임

➢ 음성인식 관련 국내 특허 동향

- 음성인식 기술과 관련된 국내 특허는 특허청 검색 결과 약 12,000여건 정도가 조사되었으며 그 중 LG전자와 삼성전자가 3,500여건의 가장 많은 특허를 보유하고 있으며, 그 외에 SKT와 KT가 250여건과 200여건을, ETRI 또한 약 200여건의 특허를 보유하고 있음

- 그러나 원거리 환경에서의 음성인식에 관련된 특허는 총 500여건 정도로 낮은 비율을 차지하고 있는 것으로 나타남
- 대화처리와 관련된 특허 건수는 약 3,400여건으로 조사되었으며, 마이크로소프트, LG전자, 삼성전자가 각각 200여건 정도의 특허를 보유하고 있으며, 그 뒤로 ETRI, 퀄컴 등이 100여건 정도의 특허를 보유하고 있음

2. 해외 기술 동향

➢ 인공지능 기반의 음성인식 시장 확대

- 영어 기반의 음성 인식은 상당부분 진척이 되어 있는 상황으로 Nuance, Verint 등 전문업체들이 미국 등 선진국에서 사업화를 진행하고 있음
- 음성 대화의 경우, 애플 SIRI, 아마존 ECHO, MS Cortana 등을 통해 글로벌 서비스가 진행되고 있으며, 이를 콜센터와 같은 기업-고객 상담 시장에 적용하려는 업체(Nuance 등)가 증가하고 있음

➢ 음성인식 관련 해외 특허 동향

- 최근 음성인식 분야의 국외 특허 출원은 Google, Microsoft, Facebook, Nuance와 같은 글로벌 기업이 대다수를 차지하고 있는 실정임
- Facebook은 자동 음성통역 분야에 특화된 자연어 음성인식 기술을 확보하고 있으며, Nuance는 인식 대상의 대화체 음성인식 기술 및 고객을 위한 인식엔진 특화 기술을 확보 중임
- 대화처리 분야의 경우, 언어 이해 및 사용자 의도 파악과 관련된 특허가 Nuance, AT&T를 중심으로 출원되고 있음

3. 기술적 경쟁력

경쟁기술	본 기술의 우수성 및 차별성
BeamFormIt (ICSI, Berkley Univ., 2014)	- 장점: 실시간성, 구현 용이, 정상잡음 감쇄에 효과적, DB 없음(비학습 기반) - 단점: 마이크 배열의 정보를 요구, 비정상 잡음 감쇄 효과가 떨어짐 - 비교우위: 마이크의 배열 정보 불필요, 잡음모델 학습 기반이므로 다양한 비정상 잡음 감쇄에 효과적
SNMF+ONL (GIST, 2016)	- 장점: 실시간성, 정상 및 비정상 잡음 감쇄에 효과적, 소용량의 음성 DB만 요구 - 단점: 다채널 처리에 용이하지 않음, 음원 분리에 따른 음질 열화 발생 - 비교우위: NTF를 이용하여 임의의 다채널 오디오에서의 음성 분리에 적합, 딥러닝 기반의 IRM 추정치를 원신호에 적용하므로 음질 열화를 개선
SEGAN (Universitat Politecnica de Catalunya, 2017)	- 장점: End-to-End 훈련 기반, 고품질의 잡음 감쇄, 다양한 잡음환경 대응(DB가 충분히 큰 경우) - 단점: 다채널 구조 변경이 매우 어려움(네트워크 구조 재도출 필요), 실시간성 x, 다량의 음성 및 잡음 DB 요구 - 비교우위: 실시간성, 다채널 활용을 통한 고품질 음성 분리 가능, 소용량 음성 DB만으로 구현 용이

4. 제품화 및 활용 분야

활용 분야(제품/서비스)	제품 및 활용 분야 세부내용
AI speaker	다채널 마이크로폰의 음질개선을 통한 음성인식 성능 향상
Mobile Phone	음질개선을 통한 통화 품질 개선
보안용 IoT	잡음제거를 통한 음향 기반 사건 검출의 성능 향상

IV. 기대효과

1. 기술도입으로 인한 경제적 효과

➢ 본 기술은 다양한 환경에서의 잡음에 적용이 가능하며, 소프트웨어 솔루션으로 음질 개선은 물론이고, 음성인식 시스템의 성능 향상에 기여

2. 기술사업화로 인한 파급효과

➢ 다양한 환경에서의 스마트 디바이스 등에 활용되어 현재 인공지능 기술과 관련하여 가장 이슈가 되고 있는 음성인식 응용 서비스에 지원함으로써 다양한 기업들이 각자의 목적에 맞는 서비스를 쉽게 구축할 수 있음

주간기술동향 원고 공모

정보통신기획평가원은 주간기술동향의 ICT 기획시리즈에 게재할 **"스마트시티"** 분야 원고를 모집하고 있습니다.

관심 있는 전문가 분들의 많은 참여를 바랍니다.

❑ 원고 주제 : **스마트시티 관련 기술·시장·정책 동향**
(※ 제목과 목차는 저자가 자율적으로 결정)

❑ 제출 자격 : 대학, 연구기관, 산업체 재직자

❑ 접수 기간 : **2019년 9월 1일~10월 31일 기간 내 수시접수**

❑ 제 출 처 : 주간기술동향 원고접수메일(wttrends@iitp.kr)로 제출

❑ 원고 양식: 파일참조(원고양식)

❑ 원고 분량: 13페이지 내외

❑ 기타

- 게재 원고에 대하여 소정의 원고료 지급(200자 원고지 10,000원/1매, 최고 40만 원)
- 기획시리즈 칼럼은 매주 1편씩 발간 예정
- 원고제출 시 반드시 원고심의의뢰서(첨부파일참조)를 함께 제출하여 주시기 바랍니다.
- 게재된 원고로 인해 지적재산권 침해문제가 발생할 경우, 원고저자는 원고료 반환, 게시물 삭제 및 정보통신기획평가원이 입게 될 손실·비용에 대한 배상 등의 불이익을 받을 수 있습니다.

❑ 제출 및 문의처

- (34054) 대전광역시 유성구 화암동 58-4번지 정보통신기획평가원
기술정책단 산업분석팀 주간기술동향 담당
- Tel : 042-612-8296, 8214 / Fax : 042-612-8209 / E-mail : wttrends@iitp.kr

IITP 정보통신기획평가원

- 사업책임자: 문형돈(기술정책단장)
- 과제책임자: 이성용(산업분석팀장)
- 참여연구원: 이재환, 이효은, 이상길, 안기찬, 김용균, 정해식, 김우진, 장예지, 전영미(위촉)

주간기술동향

통권 1915호(2019-37)

발 행 년 월 일 : 2019년 9월 25일
발 행 소 : IITP 정보통신기획평가원
편집인겸 발행인 : 석제범
등 록 번 호 : 대전 다-01003
등 록 년 월 일 : 1985년 11월 4일
인 쇄 인 : ㈜승일미디어그룹

IITP 정보통신기획평가원

(34054) 대전광역시 유성구 유성대로 1548(화암동 58-4번지)
전화 : (042) 612-8296, 8214 팩스 : (042) 612-8209

깨끗한 IITP, 신뢰받는 IITP

IITP 정보통신기획평가원

http://www.iitp.kr

IITP 부정비리 신고센터