특허청 kista 한국특허전략개발원

한국특허전략개발원
[본원] 대전광역시 중구 대종로 540 유안타증권빌딩 14층, 15층 (34831)
[분원] 서울시 강남구 테헤란로 131 한국지식재산센터 8층 (06133)
http://biz.kista.re.kr/epcenter

QR코드 찍고
전문지를 만나보세요.

국민의 내일을 위한 정부혁신
보다 나은 특허청

SEP Inside 표준특허 전문지

Standard Essential Patent

ISSN 2289-0696 (online)
ISSN 2465-9231 (print)

Theme / 양자 내성 암호(Post Quantum Cryptography)

Vol.36
2022. 12

특허청 kista 한국특허전략개발원

스마트하게
SEP Inside를 만나보세요!

SEP Inside
표준특허 전문지

Vol.36 2022. 12

CONTENTS

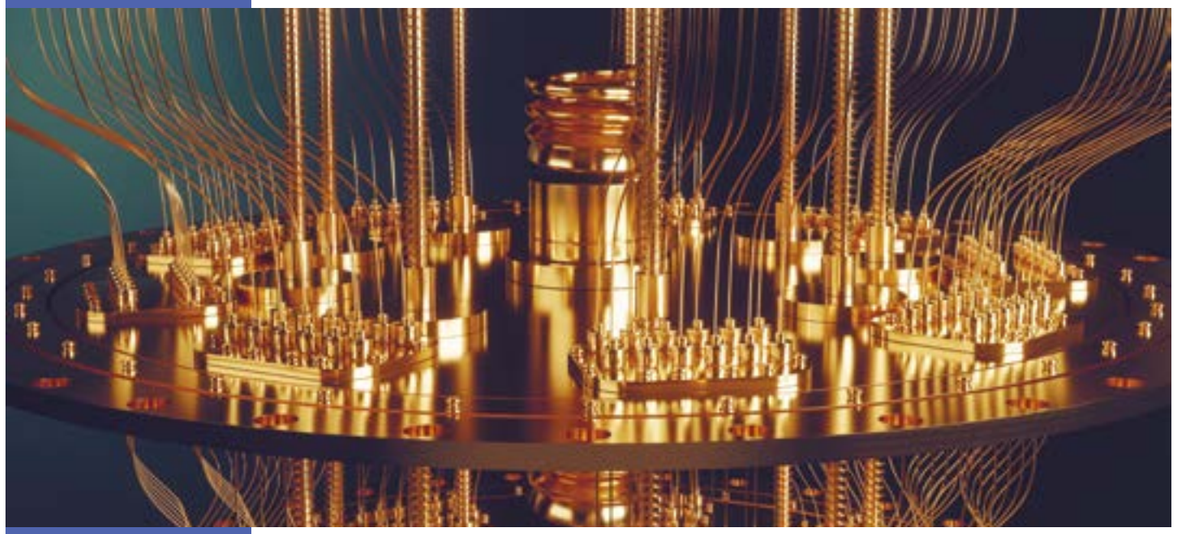
양자내성암호(PQC) 기술 개요 및 NIST 공모전 동향

한국인터넷진흥원
김기문 팀장

1 개요

1) 양자컴퓨터 및 양자 알고리즘의 발전

1994년 피터 쇼어(Peter Shor)에 의해 양자 연산으로 소인수분해 문제를 다항식 시간(Polynomial time)으로 해독할 수 있는 알고리즘이 소개된 이후 양자 컴퓨터를 구현하기 위한 연구가 진행되었다. 오늘날 양자 컴퓨터 구현 기술이 Google, MS, Intel, IBM 등 대표적인 IT 기업들을 중심으로 빠른 속도로 발전하고 있으며, 최근에는 이미 특정 문제에 대해 슈퍼컴퓨터 성능을 뛰어넘은 것으로 평가되고 있다. 따라서 현재 광범위하게 응용되고 있는 RSA와 타원곡선 암호(Elliptic Curve Cryptography) 기반의 암호화 및 전자서명 알고리즘을 해독할 수 있는 수준의 양자 컴퓨터가 앞으로 10년 이내에 등장할 것으로 예상된다.



이러한 문제에 대응하기 위해 양자 컴퓨터상에서의 연산에서도 안전한 새로운 암호 알고리즘에 관한 연구가 활발하게 이루어지고 있으며 이런 암호 기술을 양자 내성 암호(quantum safe cryptography) 또는 양자 컴퓨터 이후에도 안전하게 사용할 수 있는 암호라는 의미의 포스트 양자 암호(Post Quantum Cryptography: PQC)라 부른다.

표 1 양자내성암호 기반문제별 설명 및 특징

기반문제	설명	특징
격자	수학적 격자 구조에서 비밀 벡터를 찾는 문제	- 가장 범용적인 기반문제 - PKE/KEM, 전자서명 모두 사용
코드	비밀 행렬로 구성된 선형 코드의 디코딩 문제	- 특이 애플리케이션에 적합 - PKE/KEM 위주 사용
다변수	비밀 성분으로 구성된 다변수 이차방정식 문제	- 특이 애플리케이션에 적합 - 전자서명 위주 사용
해시함수	암호학적 해시함수의 충돌쌍을 찾는 문제	- 높은 안전성을 보유 - 전자서명에만 사용
아이소제니	타원곡선 간의 비밀 관계 연산을 찾는 문제	- 특이 애플리케이션에 적합 - PKE/KEM 위주 사용

이런 활동에 부응하여 미국 연방정부의 표준 기술을 제정하는 NIST(National Institute of Standards and Technology)에서는 2016년 포스트 양자 암호 알고리즘 표준화를 위한 알고리즘 공모전을 공지하였고, 2017년 11월에 82개의 알고리즘을 접수하여 본격적으로 표준화 과정을 진행하고 있다.

2) NIST PQC 공모전

NIST PQC 공모전은 최초에 PKE(Public Key Encryption), KEM(Key Encapsulation Mechanism) 그리고 전자서명(Digital Siganture) 알고리즘 등 세 가지 트랙이 동시에 진행되는 방식으로 공지되었으나, 진행 과정 중에 PKE만으로 제안된 알고리즘이 매우 적고, PKE를 기반으로 한 KEM 알고리즘이 다수를 차지하여 실제 진행 과정에서는 PKE와 KEM을 하나의 트랙으로 나머지 전자서명 알고리즘을 다른 트랙으로 구분하여 진행하였다. 2017년 마감된 알고리즘 제안에서는 총 82개의 알고리즘이 제안되었다. 이 중에서 기본 요건 및 특성을 NIST에서 자체 분류하여 67개의 알고리즘을 1라운드 대상 알고리즘으로 선별하여 공표하였다.

2018년 4월에는 1라운드 알고리즘 제안자 발표를 진행하였으며, 2019년 1월에 2라운드 선정 알고리즘이 발표되었으며, 2019년 8월에 2라운드 알고리즘 제안자 발표 및 워크숍을 진행하였다. 마지막으로 2020년 7월에 최종적으로 3라운드 알고리즘이 발표되었다. [표 2]에서는 NIST PQC 표준화 과정 중 라운드별 선정된 알고리즘을 종류별로 분류하였다. [표 2]의 3라운드 알고리즘에서 숫자는 본 알고리즘 수를 의미하고 괄호 안의 숫자는 후보 알고리즘으로 공개된 알고리즘 수를 의미한다.

NIST에서는 제안 알고리즘들의 보안 수준이 사전에 정의된 다섯 가지 영역(Exhaustive Key Search : AES-128, AES-192, AES-256 / Collision Search : SHA-256, SHA-384)에 맞추도록 요구하였다.

표 2 NIST PQC 표준화 라운드별 알고리즘 분류

	PKE/KEM			전자서명			소계	비율
	1라운드	2라운드	3라운드	1라운드	2라운드	3라운드	3라운드	3라운드
Code	17	7	1(2)	3	0	0(0)	1(2)	20%
Lattice	21	9	3(2)	5	3	2(0)	5(2)	47%
MQ	2	0	0(0)	7	4	1(1)	1(1)	13%
SIDH	1	1	0(1)	0	0	0(0)	0(1)	7%
Hash	0	0	0(0)	3	1	0(1)	0(1)	7%
Others	5	0	0(0)	2	1	0(1)	0(1)	7%
총계	46	17	4(5)	20	9	3(3)	7(8)	100%

이를 통해 제안된 알고리즘 사이의 성능 비교를 위한 기준을 마련하였으며, 보안과 성능 사이의 절충 관계를 고려해 제안자들이 해당 파라미터를 제안할 수 있었다. 또한, 공개키 암호와 KEM 방식에서는 최소 IND-CCA2 (Indistinguishability under adaptive chosen ciphertext attack) 안전성을 만족해야 하며 특별한 경우에 IND-CPA (Indistinguishability under chosen-plaintext attack) 안전 조건을 만족하는 것을 허용하였다. 전자서명의 경우에는 EUF-CMA(Existentially unforgeable under adaptive chosen message attacks) 안전 조건을 만족할 것을 요구하고 있다.

기존 NIST의 암호 표준화와 가장 큰 차이점은 이번 표준화 과정에서는 단일한 알고리즘 선정이 아닌 여러 알고리즘을 포트폴리오 형식으로 선정할 예정이라는 점이다. 최종 3라운드에는 최종 3라운드 알고리즘 이외에 대체 가능한 후보 알고리즘이 함께 공개되었다. PKE/KEM 분야에서는 총 4개의 알고리즘이 3라운드 알고리즘으로 선정되었고, 전자서명에서는 총 3개의 알고리즘이 선정되었다. 가장 눈에 띄는 점 중 하나는 선정된 알고리즘이 모두 서로 다른 수학적 난제에 기반을 두고 있다는 것이다. 이는 양자 내성 암호의 안전성에 대해 완전한 확신을 하지 못하는 상황에서 현재 어려운 문제가 향후 효율적인 연산 방법이 발견되어 공격이 이루어진다 하더라도, 다른 문제에 기반을 둔 또 다른 알고리즘을 통해서 표준이 바로 무력화되지 않도록 만들고자 하는 의도가 담겨 있다. 마찬가지 이유에서 대체 가능한 후보 알고리즘 역시 3라운드 알고리즘에서 향후 새로운 암호 해독 기술이 발견되더라도 후보 알고리즘에서 대체할 수 있도록 하였다.

3라운드 알고리즘을 선정할 때 가장 중요한 기준은 보안이었다. 평가 과정에서 기존에 조금이라도 보안 이슈가 있는 알고리즘들은 대부분 배제가 되었으며, 반대로 오랫동안 안전성을 인정받은 McEliece와 NTRU와 같은 알고리즘들이 최종 후보에 포함되었다. 또한 TLS, SSH, IKE(Internet Key Exchange), IPSec, DNSSEC 등 다양한 인터넷 프로토콜들과 연동 가능성도 중요한 평가 기준 중 하나였다.

보안을 위한 기준은 앞서 언급한 대로 PKE/KEM은 IND-CCA2를 만족하도록 하며 IND-CCA2보다 더 쉬운 보안 가정인 IND-CPA의 경우에는 일회용 사용의 경우 사용이 허용되었다. 전자서명의 경우 EUF-CMA를 만족시키는 알고리즘을 선정하였다. 보안 수준 난이도에 따라 5가지로 정해졌지만, 처음 세 개의 난이도 1, 2, 3이 중심이 되고 4와 5는 옵션으로 허용 되었다.

이후, NIST에서는 22년 7월에 양자내성암호 공모전 3라운드를 완료하여 최종선정 알고리즘 4종과 다양성을 넓히기 위한 4라운드 진출 알고리즘 4종에 대하여 발표하였다. 최종선정 알고리즘은 PKE/KEM 분야의 격자기반 CRYSTALS-KYBER, 전자서명 분야의 격자기반 CRYSTALS-Dilithium, Falcon, 해시기반의 SPHINCS+가 선정되었다. 최종선정 알고리즘의 분포가 격자기반이 다수임에 따라서 격자기반의 의존도를 낮추기 위하여 코드기반 및 아이소제니 기반 등으로 확대하여 약 1년간 4라운드를 진행할 계획이다.

4라운드까지 평가가 끝난 후에는 최종적으로 다음과 같이 두 가지 기존의 표준 문서에 대한 보충 알고리즘으로 PQC 알고리즘들이 포함될 예정이다. 우선 전자서명의 경우는 기존의 FIPS 186-4 Digital Signature Standard(DSS)에 추가될 예정이다. KEM의 경우에는 SP800-56B에 추가될 예정이다

2 최종선정 알고리즘

1) CRYSTALS-KYBER

CRYSTALS라는 이름으로 두 개의 알고리즘이 제안되었는데, 그 중 KEM 방식으로 제안된 것이 KYBER이고 전자서명으로 제안된 것이 DILITHIUM이다. CRYSTALS 방식은Ring-LWE(Learning With Error)를 일반화시킨 Module-LWE 기반 암호로서 LWE를 사용한 암호화 방식을 처음으로 제안한 Regev의 암호화 알고리즘을 응용한 방식이라 할 수 있다. KYBER는 Fujisaki-Okamoto 변환을 통해서 IND-CCA2 조건을 달성하였으며, QROM(Quantum Random Oracle Model)을 기반으로 보안 증명을 제시하였다. 또한, cyclotomic ring을 사용하였기 때문에, NTT (Number Theoretic Transform)를 사용해서 효율적으로 구현할 수 있다. 매우 작은 파라미터 크기를 가지며 대부분의 사용 환경에서 좋은 성능을 보여주고 있다. Module의 rank와 LWE의 noise 파라미터를 사용해서 성능을 조정할 수 있다. 그러나 Module-LWE 문제에서 SVP(Shortest Vector Problem)로의 reduction이 증명되었지만, KYBER 같은 알고리즘에 그대로 적용하기 어려운 문제가 있다. 최근에 난수(Nonce)를 재사용하는 경우에 대한 오류 주입 공격이 알려져 부채널 공격 이슈가 발생했으나, 이 문제는 모든 LWE 방식에 공통적으로 적용될 수 있는 것으로 KYBER만의 문제라고 할 수는 없다. 라운드가 바뀌면서 제안자들이 알고리즘을 수정할 기회를 주었으나 KYBER의 경우는 SHA3-256을 SHAKE256으로 교체한 것을 제외하면 변경된 것이 없을 정도로 매우 안정적인 알고리즘이라 할 수 있다.

2) CRYSTALS-DILITHIUM

CRYSTALS-DILITHIUM은 KYBER와 기본 특성 및 구조를 공유하는 Module LWE를 사용하는 격자 기반의 전자서명 알고리즘이다. 이 알고리즘은 Module LWE와 Module SIS(Short Integer Solution) 문제의 어려움에 기반을 두고 있으며 Fiat-Shamir with abort 방식을 사용하고 있다. 모든 파라미터에서 동일한 Ring 구조와 Modulus를 사용함으로써 경쟁 알고리즘 및 FALCON 대비 더 단순한 구현이 가능하다. 키의 길이와 서명의 길이 그리고 키 생성 알고리즘, 서명 알고리즘, 검증 알고리즘에서 다른 경쟁 알고리즘 대비 우수한 특성을 보여주고 있다. 특히, 2라운드 과정에서 알고리즘을 더욱 효율적으로 구현할 수 있는 방법이 제시되었고, QROM에 대한 보안 분석이 DILITHIUM에 잘 적용된다.

표 3 전자서명 알고리즘의 사이즈(Key/Signature) 및 소요시간(서명생성/검증)

Algorithm	NIST Verdict	Approach	Private Key	Public key	Signature	Sign/s	Verify/s
Crystals-Dilithium-II [29]	Finalist	Lattice	2.8kB	1.2kB	2.0kB		
Falcon-512[31]	Finalist	Lattice	57kB	0.9kB	0.7kB	3,307	20,228
Rainbow-I_a[56]	Finalist	Multivariate	101kB	158kB		8,332	11,065
RedGeMSS128[16]	Candidate	Multivariate	16B	375kB		545	10,365
Sphince$^+$-Haraka-128s[11]	Candidate	Hash	64B	32B	8kB		
Picnic-L1-FS[17]	Candidate	Hash	16B	32B	34kB		
Picnic2-L1-FS[17]	Candidate	Hash	16B	32B	14kB		
EdDSA-Ed22519[12]		Elliptic curve	64B	32B	64B	25,935	7,954
ECDSA-P256[12]		Elliptic curve	96B	64B	64B	40,509	13,078
RSA-2048[12]		Prime	2kB	0.3kB	0.3kB	1,485	49,367

3) FALCON

FALCON은 Hash-and-Sign 기반의 격자 기반 전자서명 알고리즘으로 NTRU 격자 상에서의 SIS문제의 어려움에 기반을 두고 있다. ROM(Random Oracle Mode)/QROM 기반의 보안 증명을 제공하며 전자서명 알고리즘 후보 중에서 가장 작은 파라미터 크기를 갖고 있다는 장점이 있다. 효율적인 서명 알고리즘, 검증 알고리즘 성능을 보여주고 있기 때문에 실제 응용에서도 준수한 성능을 보여주고 있다. 2라운드에서 Category 3에 해당하는 파라미터가 새로 제공되었으며 알고리즘이 단순화되었다. 또한, 부채널 공격에 내성을 갖도록 상수 시간의 알고리즘이 2라운드 기간 동안 제시되었다. 그러나 알고리즘 내부의 트리 구조, 과도한 부동소수점 연산, 이산 Gaussian 분포로부터의 랜덤 샘플링을 사용하면서 경쟁 알고리즘인 CRYSTAL DILITHIUM 보다는 좀 더 복잡한 알고리즘을 갖고 있으며, 또한 키 생성 알고리즘이 비교적 느린 편이다.

4) SPHINCS+

SPHINCS+ 알고리즘은 Stateless Hash 기반의 전자서명 방식으로 해시 함수의 보안에 의존하는 방식으로, ROM 기반의 보안 증명을 제시하고 있다. 해시 함수 기반의 전자 서명도 타원 곡선 암호보다 더 이전에 소개된 서명 방식이라 그 이후로의 많은 공격에서 살아남았고 그에 따라 알고리즘 기반 문제는 이미 충분한 신뢰성을 확보하고 있다고 할 수 있다.

2 최종선정 알고리즘

전 세계 국가 및 글로벌 빅테크 기업 등에서 양자컴퓨터에 대한 연구가 활발하게 진행됨에 따라서 RSA, ECC와 같은 기존의 공개키 암호알고리즘이 향후 해독될 수 있을 것이라는 우려가 확산되고 있다. 기존의 암호기술은 인터넷과 모바일의 발달로 거의 모든 ICT 환경에서 데이터보호, 지불결제, 신원인증 등 기능을 제공하며 대면 사회에서 비대면 사회로의 안전한 패러다임 전환에 큰 몫을 하여왔다.

이러한 현재 상황들로 인해 암호학계 및 각국 정부에서는 양자컴퓨터에도 안전한 암호(quantum safe) 또는 양자 컴퓨터에 대해서도 내성을 갖는(quantum resistant) 새로운 암호에 대한 연구 및 전환을 고려한 대책 마련 등 분주하게 움직이고 있다.

특히, 미국에서는 양자 내성 암호 전환 워크숍('20.10)을 시작으로, 전환 시나리오('21.6), 전환 로드맵('21.10)을 발표하였고, 최근 미 바이든 정부에서는 "미국을 양자컴퓨터 위협으로부터 보호하기 위해 IT 인프라를 양자 내성 암호로 전환하는 프로세스를 시작해야 한다."라는 행정명령('22.5)까지 내리면서 전 세계 어느 국가보다 가장 빠르게 준비하고 전환을 시작하였다. 유럽, 일본, 중국 등 다양한 국가들도 미국을 예의주시하며 각 국가별 상황에 맞춘 전환계획 및 시범적용 계획 등을 마련 중이다. 국내에서도 KPQC 연구단 발족을 통해 국산 양자 내성 암호를 개발 및 NIST 최종 선정 알고리즘에 대한 안전성 검증 등을 추진해 나갈 계획이다. 양자 내성 암호로의 완전한 전환을 위한 소요시간이 약 10년 이상 더 걸릴 것이라는 전문가들의 의견을 감안하여, 지금부터라도 국가/공공 및 민간 기업별 준비계획을 마련하여 양자컴퓨터 환경에서도 안전한 데이터 보호 및 서비스의 제공이 될 수 있도록 철저한 준비가 필요할 것이다.

참고문헌

[1] 김영식(2020), "NIST 양자 내성 암호 표준화 3라운드 알고리즘 특성 비교", ITFIND 주간기술동향 1976호, 2020.12. pp.14-27.
[2] Bos, Joppe, et al. "CRYSTALS-Kyber: CA-secure module-lattice-based KEM." IACR Cryptology ePrint Archive 2017 (2017): 634.
[3] D. Jao, R. Azarderakhsh, M. Campagna, C. Costello, L. D. Feo, B. Hess, A. Jalali, B. Koziel, B. LaMacchia, P. Longa, M. Naehrig, J. Renes, V. Soukharev, and D. Urbanik, SIKE, Retrieved Mar. 1, 2019, https://sike.org
[4] Eric Croket, Christian Paquin, and Douglas Stebila, Prototypin post-quantum and hybrid key exchange and authentication in TLS and SSH,
[5] T. Oder and T. Gneysu, "Implementing the NewHope-Simple key exchange on Low-Cost FPGAs," in Proc. Cryptology-LATINCRYPT 2017, La Habana, Cuba, Sep. 2017.
[6] Eric Crokett, Christian Paquin, and Douglas Stebila, <Prototyting post-Quantum and hybrid key exchange and authentication in TLS and SSH>, July. 2019
[7] Joppe W.Bos, Joost Renes and Christine van Vredendaal, <Post-Quantum Cryptography with Contemporary Co-Processors> by NXP Semiconductors
[8] Bos, J., Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schanck, J. M., & Stehlé, D. "High-speed key encapsulation from NTRU." International Conference on Cryptographic Hardware and Embedded Systems, pp. 232-252. Springer, Cham, 2017.

Avanci, Stellantis NV와 특허 라이선스 계약

2022.9.21. 출처 : Avanci

2G, 3G, 4G 표준특허 라이선스 부여

Avanci는 Stellantis NV(이하 Stellantis)와 특허 라이선스 계약을 체결했다고 발표했다. 해당 계약을 통해 Stellantis는 Avanci 표준특허 풀의 2G, 3G, 4G 표준특허를 커넥티드카에 사용할 수 있게 되었다. 이에 Avanci의 창업자 겸 CEO인 Kasim Alfalahi는 "Avanci는 세계 최고의 자동차 제조업체이자 모빌리티 공급업체인 Stellantis를 라이선스 제공자로 맞아 매우 기쁘다"라고 말했다.

Avanci는 라이선스를 공유하는 방식으로 차량 기간 내 고정 요율을 내면 특허 보유자의 지적 재산에 대한 라이선스를 반복하여 사용할 수 있을 수 있다. Avanci는 기술 공유 프로세스를 간소화하여 자동차 제조업체에 커넥티드 차량에 필요한 셀룰러 기술을 연결하며 1억 대 이상의 차량이 현재 Avanci에 의해 라이선스를 제공받는다.

VVC 특허풀 라이선스 프로그램 지원

2022.10.7. 출처: MPEG LA, 전자신문

VVC 특허 포트폴리오 라이선스 채택을 지원하기 위한 공표

MPEG LA, LLC는 국제표준특허 특허사용 계약 전문회사인 Access Advance 국제표준특허 풀 'VVC Advance'(이하 VVC)에 대한 라이선스를 발표했다. VVC는 4K에서 16K의 및 360도 영상을 모두 지원할 수 있는 차세대 영상 압축 기술로 2020년 7월에 개발이 확정됐다.

발표안의 내용은 기술특허 사용료 면제에 관한 내용이다. MPEG LA의 VVC 라이선스 제공자는 모든 VVC 소프트웨어 제품을 인세 없이 사용할 수 있다. 또한 MPEG LA의 AVC, HEVC, VVC 특허 포트폴리오 라이선스를 체결하고 이를 준수하는 사용자는 VVC 기술특허 사용료 할인을 받는다.

ARM, 퀄컴과 누비아를 상대로 라이선스 계약 위반에 따른 소송

2022.09.13. 출처 : 한국지식재산연구원

반도체 칩 디자인 관련 특허 소송

누비아는 2019년 설립 당시 ARM과 라이선스 계약을 체결했으며, 2021년 퀄컴이 누비아 인수를 추진하면서 ARM이 퀄컴을 상대로 새로운 라이선스 협상을 요구하였으나 퀄컴이 이에 응하지 않자 소송을 제기했다.

ARM은 미국 델라웨어 지방법원에 제기한 소송에서 누비아가 반도체 칩 디자인의 폐기를 요구하고, ARM의 동의 없이 누비아의 라이선스를 퀄컴에 양도할 수 없다고 주장했다. 2019년 ARM은 자사가 누비아에 라이선스를 제공한 '명령어 집합체(이후 ISA)'를 활용해 누비아의 CPU가 설계되었다고 밝혔다. 2021년 퀄컴의 누비아 인수로 퀄컴 측에 자사의 승인 없이 누비아가 취득한 라이선스를 사용할 수 없음을 통보하였고, 새로운 라이선스 협상을 했다. 동 소송은 ARM 주 메모리인 ISA 반도체를 개발하는 *오픈소스 소프트웨어 권리에 대한 소송이다.

* 오픈소스 소프트웨어(Open Source Software, OSS)는 관련 저작권자가 누구든지 어떤 목적으로든 학습, 수정, 배포할 수 있는 권한을 제공하는 라이선스로 이루어진 소스코드의 소프트웨어를 의미함.

SISVEL, Cellular IOT 특허 풀 출시

2022.11.9. 출처: SISVEL

표준 필수 특허(SEP)에 라이센스를 부여하는 단일 솔루션 제공

SISVEL은 Cellular IoT(이하 C-IoT) 기술에 대한 특허풀 출시를 발표했다. C-IoT 특허풀은 ASUSTek, Datang, Ericsson, ETRI외에 20개의 기업이 특허풀에 합류했다. C-IoT의 이점은 전자 정보(ex. 전력 소비량, 전압 레벨) 계량기의 처리량 증가와 자산 추적 속도 향상이다. 라이선스 조건은 다음과 같다. 대부분의 IoT 제품의 경우 요금은 단위당 0.6달러이며, LTE 기능이 추가된 IoT 기술의 경우 스마트 계량기 기능은 단위당 2달러, 자산 추적 기능은 단위당 1.33달러이다.

Cellualr IoT 특허 풀을 생성함으로써 참여하는 특허 소유자는 LTE-M 및 협대역 IoT 표준을 구현하는데 필요한 모든 단일 특허를 공유한다.

뮌헨 법원, 애플이 에릭슨을 상대로 제기한 특허 무효 소송 기각

2022.10.12. 출처: FOSS PATENTS, 전자신문

2021년 특허 라이선스 계약 종료로 시작된 분쟁

2015년 Apple이 Ericsson의 5G 지원 기능을 사용함에 따라 양사의 파트너 관계가 시작되었지만, 2021년 특허 라이선스 계약 종료와 함께 로열티 문제로 상호 소송전에 돌입했다. 에릭슨은 애플이 라이선스 계약 갱신을 하지 않고 특허를 무단 사용하고 있다는 주장을, 애플은 에릭슨이 세계적으로 부당하게 과도한 로열티를 요구하고 있다는 주장으로 입장을 대립하고 있다.

소송 중인 *특허는 "인터넷 기반 애플리케이션에 대한 모바일 액세스"에 관한 기술이다.

* EP2220848

UKIPO, 표준필수특허(SEP)에 대한 전문 의견 수렴

2022.8.23. 출처: https://www.gov.uk, 한국지식재산연구원

5G 및 셀룰러 기술과 같은 무선 기술의 관심 향상

영국 정부는 SEP의 생태계가 효율적으로 기능하여 관련된 모든 주체에 대해 올바른 균형을 이루고 있는지에 대한 증거를 수집하고 정부 개입이 필요한지를 평가하기 위해 2021년 12월부터 2022년 3월까지 12주간 공중에게 의견 제출을 요청했다. 그 결과, 통신, 자동차, 기술 산업, 학계, 법률 및 IP 전문직 등의 분야에서 총 56개의 서면 의견이 수렴되었다.

동 발표의 주요 내용은 다음과 같다.

- 통신, 자동차, 사물인터넷(IoT) 부문에서 3G, 4G, 5G와 같은 무선 기술의 사용이 증가함에 따라 특허 특허사용 계약과 표준 사용에 관한 관심이 높아지고 있음
- 수렴된 의견은 ① SEP, 혁신 및 경쟁 간의 관계와 어떠한 조치 또는 개입이 영국 소비자에게 가장 큰 개선을 가져올 것인지, ② 경쟁과 시장 기능, ③ 시스템의 투명성, ④ 특허 침해 및 구제, ⑤ SEP 라이선스, ⑥ SEP 소송의 총 6가지 주제로 요약됨

MPEG LA의 전기 자동차 충전 라이선스 포트폴리오 향상

2022.11.17. 출처: MPEG LA

MPEG, EV 전기자동차 시스템 라이선스 포함

2022년 11월 17일, MPEG LA는 GE Hybrid Technologies, 미쓰비시 중공업, Robert Bosch, Siemens 기업을 MPEG LA의 EV 충전 특허 포트폴리오 라이선스 제공자로 추가로 포함했다. 해당 라이선스 제공자는 자신과 그 계열사가 라이선스 또는 재라이선스할 권리가 있는 모든 EV 충전 필수 특허를 포함하는 데 동의한다.

MPEG LA의 EV 충전 특허 포트폴리오 라이선스는 전기자동차에 전기 충전을 제공하는 장비에 사용되는 전도성 AC 및 DC 충전, 연결, 통신 및 안전에 대한 전 세계 표준의 기본 기술에 대한 액세스를 제공한다.

포스트 양자 암호 알고리즘 설명과 표준화 동향

조선대학교

김영식 교수

1 서언

오늘날 공개키 암호는 인터넷 보안 사물인터넷 보안 및 정보기기 시스템 보안을 위한 인증, 암호화 및 키 교환 알고리즘으로 광범위하게 활용되고 있다. 대표적인 공개키 암호 알고리즘은 1977년에 개발된 큰 정수의 소인수분해의 어려움에 기반을 둔 RSA 알고리즘 및 이산로그 문제에 기반을 둔 미국 표준 전자서명인 DSA, 타원곡선암호(ECC) 기반 문제에 기반을 둔 암호화, 서명, 및 키 교환을 위한 알고리즘이 있다.

1994년 피터 쇼어(P. Shor)에 의해서 양자컴퓨터 상에서 동작하는 소인수분해 문제와 이산로그 문제를 빠르게 계산할 수 있는 양자 알고리즘이 처음 등장하면서, RSA 및 DSA 그리고 ECC와 같은 암호는 양자컴퓨터가 실용화되면 사용할 수 없는 알고리즘이 되었다. 따라서 오늘날 실제 활용되는 주요 알고리즘이 모두 양자컴퓨터로 해독이 가능한 상황이 되었고, 최근 전 세계 주요 IT 기업들이 양자컴퓨터 개발에 박차를 가하면서 양자컴퓨터에서 비롯된 이런 위협이 현실이 되는 상황이다.

이에 대응하기 위해 양자컴퓨터 상에서의 연산에서도 안전한 새로운 공개키 암호에 관한 연구가 전 세계적으로 활발히 진행되었다. 이런 연구를 양자 내성 암호 또는 양자컴퓨터 이후에도 안전한 암호라는 의미의 포스트 양자 암호(Post-Quantum Cryptography)로 부른다. 2006년 PQC와 관련된 전문 학술대회가 처음 개최되면서 관련 연구를 수행하는 학자들이 새로운 형태의 양자 내성 암호에 대한 연구를 발표해 왔다. 한동안 암호학자들 사이에서만 연구가 진행되었으나 양자컴퓨터 구현 기술의 발달에 따라 2015년 미국 NSA에서 양자 내성 암호 기반 체계로 전환한다고 공식 발표하였고, 2016년에서는 미국 NIST에서 PQC 미국 표준을 선정한다고 공고하면서 연구에 관한 관심이 큰 폭으로 증가하였다. 그리고 미국 NIST는 PQC 표준을 2017년부터 시작하여 2022년 7월에 실제 표준 알고리즘을 선정하기에 이르렀다[1),2)]

2 PQC의 종류 및 특성

PQC에 대해 이해하기 위해서는 먼저 양자 양자 암호와 구분할 필요가 있다. 양자 암호는 이름대로 양자 현상에 기반을 둔 새로운 형태의 보안 기술로 대표적으로 양자 상태로 키를 전달하는 양자 키 분배(QKD; quantum key distribution) 기술이 실용화 단계에 있는 기술이다. QKD가 동작하기 위해서는 양자를 다룰 수 있는 별도의 하드웨어들이 필요하다. 그러나 양자를 이용한 전통적인 것과 유사한 형태의 암호화나 서명 등은 아직은 이론적 수준에 머물러 있다. 따라서 QKD를 통해서 양자적으로 안전하게 키를 전송하고 난 후에 해당 키를 사용해서 AES와 같은 전통적인 방식의 블록 암호를 사용해서 메시지를 암호화해 전송하는 방식을 취하고 있다.

반면에 포스트 양자 암호는 기존 암호들과 마찬가지로 모든 알고리즘이 별도의 하드웨어 없이 일반 범용컴퓨터상에서 동작할 수 있으며, 최근에 나온 알고리즘들은 사물인터넷 센서나 액추에이터와 같은 장치에서도 동작이 가능할 정도의 경량 연산을 사용한다.

PQC의 안전성을 이해하기 위해서는 양자컴퓨터에 대한 이해가 필요하다. Shor의 알고리즘을 필두로 전통적인 공개키 암호를 해독할 수 있는 양자 알고리즘이 현재 알려진 암호들이 기반을 둔 모든 어려운 문제들을 풀 수 있는 것은 아니다. 양자컴퓨터의 장점은 일반적으로 병렬화를 통해 만일 q개의 양자비트를 오류 없이 동시에 다룰 수 있는 양자컴퓨터가 있다면 2q개의 연산을 양자 중첩의 원리에 따라 동시에 병렬로 처리할 수 있다. 따라서 양자컴퓨터는 전통 방식의 컴퓨터에 비해서 전수조사에 기반을 둔 공격을 훨씬 더 빠르게 수행할 수 있다. 여기에 더하여 양자컴퓨터 상에서 동작하는 양자 검색 알고리즘인 Grover 알고리즘을 사용하면 기존에 필요했던 연산량을 제곱근만큼 더 적은 연산으로 수행할 수 있다. 예를 들어 미국의 표준 블록암호인 AES는 기존 컴퓨터로는 공격을 위해 2128 만큼의 연산량이 필요했던 것을, 충분한 크기의 양자비트를 제공하는 양자컴퓨터를 이용한다면 264수준으로 줄이는 것이 가능하다. 그러나 양자

컴퓨터상에서 Grover 알고리즘을 사용하더라도 기존에 사용하던 키의 길이를 두 배로 증가시키면 기존과 동등한 수준의 보안을 유지할 수가 있다.

반면 앞서 언급한 Shor 알고리즘은 암호가 기반하고 있는 특정 문제를 양자적 방법을 이용해서 더 빨리 연산할 수 있도록 만들어준다. 이런 문제에는 대표적으로 앞서 언급한 소인수분해 문제, 이산로그 문제, 타원곡선기반 이산로그 문제 등이 있다. Shor 알고리즘의 경우 특징적으로 암호가 기반하는 수 체계에 내포된 숫자의 주기에 대한 정보를 양자컴퓨터를 통해서 빠르게 추출할 수 있도록 해 주며, 이 정보를 사용하면 암호 해독이 다항식 시간으로 가능해진다.

그러나 위와 같은 문제와는 전혀 다른, 여전히 양자 가속 알고리즘이 알려지지 않은 수많은 문제가 존재한다. 대표적으로 오류가 있는 선형시스템을 푸는 문제가 있다. 이런 문제에 기반을 둔 암호로 대표적으로 격자 기반 암호 및 부호 기반 암호가 있다. 또한 해시 기반 암호, 다변수 이차방정식 기반 암호, 그리고 타원곡선 Isogeny 기반 암호 등이 양자컴퓨터에 안전한 암호로 분류된다.

3 NIST PQC 표준화 과정 소개

미국 표준국 NIST는 양자 내성 암호의 표준의 필요성이 크게 대두된 2017년부터 지금까지 양자 내성 암호 표준화를 진행하고 있다. 2016년 포스트 양자 암호 알고리즘 표준화를 위한 알고리즘 제안 요청을 공지한 이후, 2017년 11월에 82개의 알고리즘을 접수하여 표준화 과정 1라운드를 진행하였다. 이후 2라운드와 3라운드의 단계를 거쳐 알고리즘들을 순차적으로 선별한 후, 마지막 15개의 후보 중에서 2022년 7월에 1차 표준 알고리즘을 선정 발표하였다[2]. 여기에 그치지 않고 4개의 알고리즘을 라운드 4의 대상 알고리즘으로 선정하여 표준 알고리즘을 추가로 선정한다고 공지한 상태이다. 또한 전자서명의 경우 기존 알고리즘 외에 새로운 알고리즘들을 새로운 후보군으로 내년 6월까지 제출하도록 제안 요청을 한 상태이다.

NIST 표준화는 총 두 개의 트랙으로 진행되었는데, 하나는 키 교환을 위한 메커니즘 KEM(Key Encapsulation Mechanism)을 선정하는 것이고, 다른 하나는 전자서명 알고리즘을 선정하는 트랙이었다. 많은 경우 KEM은 기밀성 제공을 위한 공개키 암호화로부터 만들어지므로 표준으로 선정된 KEM 방식인 CRYSTALS-Kyber는 공개키 암호로도 사용할 수 있다.

NIST에서는 보안 수준을 총 5가지로 정의하였고, 그중에 AES의 세 가지 키의 길이 128비트, 192비트, 256비트를 기준으로 이와 동등 수준의 보안을 달성하는 것을 보안 카테고리 1, 3, 5로 정의하고 SHA3 256, 384와 동등 수준의 보안을 달성하는 것을 보안 카테고리 2, 4로 정의하였다. NIST에서는 가장 중요한 평가 요소인 보안 이외에 다양한 연산 플랫폼상에서의 성능을 중심으로 평가를 진행하였다. 이 외에 되도록 기존 양자컴퓨터에 취약한 알고리즘을 모듈식으로 대체할 수 있고, 완전 순방향 보안(perfect forward secrecy) 제공, 상수시간 연산 보장 등 기본적인 부채널 공격에 대한 방어 기능, 그리고 단순성 유연성, 오용 동작 방지 기능 등을 추가적인 고려 사항으로 제안하기도 하였다.

최종적으로는 기존에 사용되는 TLS/SSH/IKE/IPSec/DNSsec 등 프로토콜에 포함되어 사용될 것이므로 해당 프로토콜과의 호환 가능성 역시 중요한 요소였다.

4 표준 선정 알고리즘 종류 및 특징

3라운드 마지막에 NIST에서 1차 KEM으로 선정한 알고리즘은 단 한 종으로 CRYSTALS-Kyber라는 이름의 격자기반 암호이다. CRYSTALS-Kyber는 격자기반 문제 중 MLWE (Module-LWE) 문제에 기반을 두고 있으며, 여러 알고리즘 중 파라미터의 크기와 연산 속도 측면에서 가장 좋은 특성이 있어 처음부터 주목을 받아온 알고리즘이다[2].

반면 1차 PQC 전자서명 표준 알고리즘은 총 세 종이 선정되었다. CRYSTALS-Dilithium과 Falcon은 모두 격자 기반 문제에 기반을 둔 서명 방식으로 기반하는 문제는 서로 다르지만 모두 구조를 갖는 격자 문제에 기반을 두고 있어, 상대적으로 작은 크기의 공개키, 개인키 그리고 서명의 크기를 갖고, 연산 속도도 비교적 빠르게 수행할 수 있다. 또 하나의 알고리즘은 매우 오래된 암호화 방식인 해시 기반 전자서명으로 설계된 SPHINCS+라는 알고리즘이다.

표 1 NIST PQC 표준화 알고리즘 현황 및 특성[1]

	알고리즘	표준상태	분류	Security	Public	Private	Signature
전자서명	Dilithium	표준	격자기반	128	1,312	2,528	2,420
				256	2,592	4,864	4,595
	Falcon	표준	격자기반	128	897	1,281	690
				256	1,793	2,305	1,330
	SPHINCS+	표준	해시기반	128s	32	64	7,856
				256s	64	128	29,792
	알고리즘	표준상태	분류	Security	Public	Private	Ciphertext
KEM	Kyber	표준	격자기반	128	800	1,632	768
				256	1,568	3,168	1,568
	Classic McEliece	4라운드	부호기반	128	261,120	6,492	128
				256	1,044,992	13,932	240
	BIKE	4라운드	부호기반	128	1,540	280	1,572
				256	5,122	580	5,154
	HQC	4라운드	부호기반	128	2,249	40	4,481
				256	7,245	40	14,469

(단위: bytes)

1) 전자서명 표준

a) CRYSTALS-Dilithium

Dilithium은 CRYSTALS라는 이름으로 Kyber와 함께 NIST PQC 표준화에 제출된 격자기반 문제 기반 서명 방식이다[3]. Dilithium은 증명자(prover)가 검증자(verifier)에게 비밀 값을 직접 드러내지 않고 비밀값을 알고 있다는 사실을 입증하는 영지식 기반 인증을 사용하여 설계되었다. 여기에 Fiat-Sharmir 변환을 통해 서명을 생성하는 널리 알려진 방식을 채용하고 있다. 이를 통해 Dilithium은 다른 모든 경쟁 알고리즘 대비 매우 효율적이면서 간단한 구현이 가능하여 주목받았고, 보안 역시 매우 안정적인 이론에 기반을 두고 있다.

상대적으로 매우 작은 파라미터의 크기와 효율적인 연산 속도 등으로 인해 거의 모든 분야에서 응용할 수 있으므로, NIST에서는 대표적인 PQC 서명 방식으로 Dilithium을 추천하고 있다.

b) Falcon

Falcon은 Gentry, Peikert, 그리고 Viakuntanathan 이 제안한 GVP 방식에 기반을 두고 효율적 구현을 위해 NTRU라는 격자기반 암호의 한 가지 방식을 결합시킨 전자서명이다[4]. Dilithium과 달리 "Hash-and-Sign"방식의 서명 방식을 사용하고, NTRU기반 문제에 기반을 두었기 때문에 LWE문제에 기반을 둔 Dilithium 방식과 차이가 있다. Falcon 역시 견고한 이론적 기반 위에서 설계된 방식으로 공개키의 길이와 서명의 길이의 합이 모든 알고리즘 중에서 가장 작은 방식으로 이런 특성으로 인해서 Dilithium과 함께 NIST에서 추가로 표준으로 선정하였다. 공개키와 서명의 크기는 블록체인 등 특정한 응용에서 거래 정보에 포함되는 값으로 크기가 작아야 전체 저장 용량에 부담을 적게 미칠 수 있으므로, 이러한 응용을 위해 추가 표준 알고리즘으로 선정하였다.

c) SPHINCS+

SPHINCS+는 서명의 길이가 길고 연산 속도가 전반적으로 느리다는 단점을 가지만 가장 오래된 형태의 서명 방식 중 하나로 가장 보수적으로 설계된, 그래서 안전성 보장을 최우선으로 취한 방식이라 할 수 있다[5]. SPHINCS+의 공개키와 개인키는 매우 짧은 특징을 갖지만 서명의 크기가 매우 큰 특성을 갖는다. 서명의 크기가 커지면 응용에 제약이 생기지만 NIST에서는 다른 두 표준 서명 알고리즘이 격자기반 문제에 기반을 두기 때문에 다양성을 염두에 두고 해시기반 암호인 SPHINCS+를 추가 표준으로 선정되었다. 이것 역시 예상을 뛰어넘은 것으로 원래 SPHINCS+는 표준 최종후보보다는 최종후보를 대체할 수 있는 대체 알고리즘 중 하나로 3라운드에 포함되었지만, 그러나 3라운드 종료와 함께 표준으로 바로 선정 발표되었다.

2) 키 교환 표준

a) CRYSTALS-Kyber

Kyber의 경우 Module-LWE문제라는 수학 문제에 기반을 둔 암호화 방식으로 공개키 암호(PKE)를 먼저 생성한 후 KEM 방식으로 변환되는 방식으로 제안되어 공개키암호와 KEM 방식으로 동시에 사용할 수 있는 방식이다[6]. 높은 수준의 보안 특성인 IND-CCA 상에서의 보안 증명이 가능하며, 특히 격자기반 암호에 대한 신뢰할 수 있고 안정화된 체계에 근거를 두고 있어서 이런 방식 암호의 보안에 대한 분석은 매우 신뢰도가 높은 것으로 평가된다. 소프트웨어 및 하드웨어 대부분 환경에서 우수한 성능을 보여주었기 때문에, 경쟁하는 다른 유력 알고리즘을 모두 제치고 유일한 KEM 방식으로 CRYSTALS-Kyber가 선정되었다. 여기에는 우수한 성능과 함께 다른 암호들이 기반을 둔 LWR, NTRU 등의 문제보다 LWE 문제가 상대적으로 더 신뢰도가 높다고 평가되어 하나만을 선정하였다.

NIST에서는 PQC 표준화 처음부터 다양성을 매우 높은 가치로 내세웠기 때문에 여러 알고리즘이 표준으로 선정될 것으로 많은 연구자가 예상하였으나, 이런 예상을 깨고 3라운드 마지막에 하나의 알고리즘만을 선정하였다. 그러나 NIST에서는 알고리즘 선정과 함께 표준화 과정을 종료하는 대신 4라운드를 개시하여 추가로 표준 알고리즘들을 선별하는 과정을 공고하였다. 여기에 포함된 알고리즘은 4라운드 후보 알고리즘 항목에서 자세히 다룬다.

3) 4라운드 키 교환 후보

a) BIKE

BIKE는 4라운드 후보에 포함된 알고리즘으로 알고리즘의 성능 및 특성이 균형있게 우수하여 많은 주목을 받는 방식이다[7]. MDPC(moderate density parity check) 부호를 사용하는 방식으로 1의 개수가 상대적으로 매우 적은 비밀값을 두 개 생성한다. 이를 희소 다항식(sparse polynomial)이라 한다. 이 중 하나의 역원을 취해 다른 희소 다항식과 곱하면, 결과적으로 랜덤한 다항식을 얻을 수 있고, 이를 공개하더라도 원래의 두 개의 희소 다항식을 복구하는 것이 어려운 문제가 된다. BIKE는 표준화 과정에서 보안 특성이 지속해서 개선되었으며, NIST에서는 알고리즘의 효율성 및 보안 특성의 개선을 좋은 요소로 보아 4라운드에서 추가로 평가해 표준 선정 여부를 결정하기로 발표하였다. 특히 표준 알고리즘이 격자기반 암호와는 전혀 다른 부호기반 암호 중 적어도 하나를 4라운드 이후 표준화하는 것으로 이미 공식화한 상태이다.

b) Classic McEliece

Classic McEliece는 1978년 처음 제시된 이후 40년이 넘는 기간 동안 심각한 손상 없이 안전성을 유지해온, 가장 신뢰도가 높은 암호화 방식 중 하나를 사용한다[8]. 따라서 NIST나 그 어떤 암호학자도 표준화 과정에서 Classic McEliece의 보안에 대해서는 어떤 문제도 제기하지 않았다. 그러나 문제는 Classic McEliece가 가진 파라미터의 크기가 다른 모든 알고리즘 대비 매우 크기 때문에 실제 응용 가능성에 여러 가지 의문과 문제 제기가 이루어졌다. 따라서 가장 높은 보안에 대한 신뢰도를 기반으로 Classic McEliece가 표준으로 선정될 것으로 예상했던 것과는 달리, NIST에서는 Classic McEliece의 응용 가능성 및 표준으로 선정될 이유를 더 논의해 달라고 요구하면서 4라운드에서 추가로 검토해야 할 알고리즘으로 Classic McEliece를 포함했다. 특히 같은 부호기반 암호 중에서 BIKE나 HQC와 같은 경쟁 알고리즘들이 더 좋은 파라미터 특성과 연산 속도를 보여주고 있으므로 Classic McEliece이 상대적으로 의문이 제기된 것도 사실이다. 더군다나 Classic McEliece의 가장 큰 장점이 모든 알고리즘 중 암호문의 크기가 가장 작다는 점도, 경쟁 알고리즘이었던 SIKE가 비슷하게 작은 암호문 크기라는 특성을 제공하였기 때문에, 장점이 되지 못하였다. 그러나 4라운드 대상 알고리즘이 발표된 직후 SIKE가 완벽하게 공격당해 사용할 수 없게 되면서 Classic McEliece의 작은 암호문 크기는 이 알고리즘만이 제공할 수 있는 독보적 특성이 되었다. 4라운드에서 Classic McEliece의 응용 분야에 대한 합의가 이루어지면 특수한 응용을 위한 표준으로 선정될 가능성이 있다.

c) HQC

HQC는 기존 부호기반 암호가 갖고 있던 여러 특성과는 전혀 다른 새로운 형태의 구조를 가진 방식이다[9]. 특히 보안 분석이나 보안이 기반을 둔 어려운 수학적 문제로 쉽게 환원되는 특성이 있어 신뢰도를 높게 평가받았다. HQC는 순회 다항식을 사용하여 키의 길이와 암호문의 길이를 McEliece 방식 대비 크게 줄일 수 있었으나 BIKE 등 다른 경쟁 방식보다는 좀 더 큰 특성을 갖고있다. 다만 기존방식과는 달리 사용하는 오류정정부호의 구조와 HQC의 보안이 완전히 분리되어 있어서 기존처럼 오류정정부호의 구조를 사용한 공격으로부터 완전히 면역되어 있다. HQC의 보안은 순수한 랜덤 부호를 사용하기 때문에 원래 부호기반 암호가 의존하는 NP-complete 문제 중 하나인 랜덤 패리티 검사 행렬 또는 다항식의 디코딩 문제의 어려움에 직접적으로 의존하는 특성을 갖는다.

5 국내 양자 내성 암호 표준화 동향

마지막으로 국내 양자 내성 암호 표준화 동향에 대해서 간단히 설명을 하고 본 고를 마무리하고자 한다. 국내에서도 2021년부터 양자 내성 암호 표준화를 위한 준비를 위해 2021년 5월 한국양자내성암호연구단(KpqC)을 발족하여 산학연 전문가 모임을 통해 양자 내성 암호 내재화 작업을 진행해 왔다. 국내에서는 미국처럼 “표준”으로 선정하는 방식보다는 공모를 통해 우수 알고리즘을 선정하는 방식으로 진행된다. 차이점은 선정된 알고리즘이 국내 “표준”의 지위를 갖는 것은 아니지만 한국암호모듈검증(KCMVP) 등의 평가에 반영할 예정이다. 2022년 초 제안계획을 제출한 알고리즘은 총 19개의 알고리즘으로 이 중에서

전자서명은 10종, 공개키암호 5건, 키 설정 4건이 제안된 상태로, 2022년 10월 말까지 본 제안이 제출되는 등 활발한 연구가 진행되고 있다.

표 2 국내 양자 내성 암호 공모전 제안 알고리즘 분류[10]

	격자기반	부호기반	다변수기반	해시기반	Isogeny	기타	계
공개키암호	1	2			1	1	5
키설정	2	2					4
전자서명	5	1	1	1	1	1	10
							19

6 마무리

오늘날 공개키 암호는 네트워크로 연결된 세상에서 신뢰를 보장하는 가장 근본적인 구성요소로 사용되지만, 양자컴퓨터의 등장으로 인해 기존에 사용하던 공개키 대부분을 대체할 필요가 생겼다. 이런 알고리즘을 양자 내성 암호 또는 포스트 양자 암호라 부르며, 본 고에서는 주요 알고리즘의 특징 및 이번에 미국 표준으로 선정 및 고려되는 알고리즘들의 특징을 설명하였다. 또한 국내에서도 양자 내성 암호 내재화를 위한 암호 공모전이 진행 중이며, 2024년까지 마무리하는 것을 목표로 하고 있다. 양자 내성 암호는 단순히 기존 공개키를 양자컴퓨터에 안전한 방식을 제공할 수 있는 것에 더하여 새로운 암호 응용 분야를 더욱 확장시킬 수 있을 것으로 기대된다.

참고문헌

[1] https://csrc.nist.gov/projects/post-quantum-cryptography
[2] G. Alagic, et al., Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process, NISTIR 8413, July 2022.
[3] V. Lyubashevsky, et al., Supporting Document of CRYSTALS-DILITHIUM Round 3 Submission, July 2020
[4] T. Prest, et al., Supporting Document of FALCON Round 3 Submission, July 2020.
[5] A. Hulsing, et al., Supporting Document of SPHINCS+ Round 3 Submission, July 2020.
[6] P. Schwabe, et al., Supporting Document of KYBER Round 3 Submission, July 2020.
[7] N. Aragon, et al., Supporting Document of BIKE Round 3 Submission, July 2020.
[8] M. R. Albrecht, et al., Supporting Document of Classic McEliece, NISt PQC Round 3 Submission, July 2020
[9] C. A. Melchor, et al., Supporting Document of HQC Round 3 Submission, July 2020.
[10] https://kpqc.or.kr/

양자내성암호 표준화 동향

한성대학교

장경배 박사과정
양유진 석사과정
임세진 석사과정
서화정 조교수

1. 양자컴퓨터의 발전사항

2019년 10월 구글이 개발한 53-큐비트 양자 프로세서가 양자 우월성(quantum supremacy)을 달성하였다는 내용의 논문이 nature에 게재되었다. 이는 생성된 난수가 진짜인지 여부를 증명하는 난제로써 슈퍼컴퓨터에서는 1만년이 걸린 반면 양자컴퓨터 상에서는 3분 20초안에 계산 가능함을 보였다. 이로써 양자 컴퓨터가 슈퍼컴퓨터의 성능을 능가할 수 있다는 것을 세계 최초로 선보였다[1].

양자 컴퓨터 개발에는 구글과 함께 IBM도 적극적으로 나서고 있다. 2020년 IBM은 양자컴퓨터 기술 개발 로드맵을 공개하였고, 2021년 11월 세계 최초로 100-큐비트를 뛰어넘는 127-큐비트 양자 프로세서 Eagle을 공개하였다. 올해에는 433-큐비트를 수행할 수 있는 양자 프로세서 오스프레이(Osprey)를 발표할 예정이다. 2023년에 공개될 예정인 Heron은 별도의 프로세서들이 실시간으로 고전적인 통신을 할 수 있게 연결해주는 제어 하드웨어를 갖춘 133-큐비트 프로세서로써 여러 개를 연결함으로써 원하는 크기로 양자컴퓨터의 확장이 가능하다. 2024년에는 다중 칩 양자 프로세서인 Crossbill과 양자 병렬화를 지원하는 프로세서에 양자 통신 링크를 내장하여 양자 통신이 가능하게 하는 Flamingo 프로세서가 공개될 예정이다. Flamingo는 462-큐비트 프로세서로, 다중칩 프로세서의 모듈식 연결을 통한 확장을 이용하여 Flamingo 프로세서가 3개 이상 연결된 형태이다. 2025년에는 양자 통신 링크가 내장되며 1,386-큐비트 프로세서 3개가 연결된 다중 칩 프로세서 Kookaburra가 공개될 예정이다[2]. [표 1]은 앞서 이야기한 IBM의 개발 로드맵을 정리한 것이다.

표 1 IBM 양자 컴퓨터 개발 로드맵, p는 연결 가능한 프로세서의 수

Category	2019	2020	2021	2022	2023	2024	2025	2026~
Processor	Falcon	Humming bird	Eagle	Osprey	Condor Heron	Flamingo Crossbill	Kookaburra	-
Qubits	27	65	127	127	1,121 133 × p	1,386~ 408	4,158~	10~ 100만

2. NIST 양자 내성 암호 표준화 진행 과정

NIST는 앞에서 살펴본 양자컴퓨터의 등장으로 인해 야기될 보안적 위협에 대비하기 위하여 2016년 2월, 양자 내성 암호 표준화를 위한 공모전을 개최하였다. 특히 전자서명과 공개키 암호화 및 키 생성 알고리즘에 대한 공모를 받았다. 총 82개의 암호가 제출되었으며 기반 문제별로 나누면 격자기반 암호 28개, 코드기반 암호 24개, 다변수 다항식 기반 암호 13개, 해시 기반 암호 4개, 그리고 기타 암호 13개로 구성된다. 이 중에서 다수의 알고리즘이 철회되면서 최종적으로 64개의 알고리즘이 공모전에 참여하게 되었다. 공모전의 1라운드에서는 안전성 관점에 주안점을 두고 평가가 진행되었다. 그 결과 총 26개의 알고리즘이 선정되었다. 기반 문제별로 통과된 알고리즘은 격자기반 암호 12개, 코드기반 암호 7개, 다변수 다항식 기반 암호 4개, 해시기반 암호 1개, 그리고 기타 암호 2개이다. 2라운드 평가에서는 안전성 외에도 알고리즘 구현 특성과 비용, 성능이 고려되었다. 또한 이전 라운드와 달리 우수하지만 추가적인 평가를 필요로 하는 대체 후보도 함께 선정되었다. 대체 후보까지 포함하여 격자기반 암호 7개, 코드기반 암호 3개, 다변수 다항식 기반 암호 2개, 해시기반 암호 2개, 기타 암호 1개로 총 15개 알고리즘이 2라운드를 통과하였다. 3라운드에서는 1개의 공개키 암호화 및 키 생성 알고리즘과 3개의 디지털 서명 알고리즘이 표준화 알고리즘으로 선정되었고, 4건의 공개키 암호화 및 키 생성 알고리즘이 후보 알고리즘으로 4라운드에 진출하였다. 표준화로 선정된 양자 내성 암호 알고리즘과 4라운드에 진출한 후보군은 [표 2]와 같다[3].

표 2 NIST 양자 내성 암호 최종 알고리즘

알고리즘 종류	표준화 알고리즘	후보 알고리즘
암호화/키 생성	CRYSTAL-KYBER	BIKE, Classic McEliece, HQC, SIKE
전자서명	CRYSTAL-DILITHIUM, FALCON, SPHINCS+	-

후보 알고리즘 중 BIKE와 HQC는 격자 기반이 아닌 범용 키 생성 알고리즘에 적합하기에 두 알고리즘 중 한 가지가 표준화 알고리즘으로 선택될 것으로 예상되고 있다. 또한, 높은 안전성을 보장하는 Classic McEliece의 경우 큰 공개키 크기로 인해 실용적으로 사용되지 못할 것으로 간주되어 3라운드에서 최종 후보였으나 표준화되지 못하고 후보 알고리즘으로 4라운드에 진출하게 되었다[3].

후보 알고리즘들의 수정본 제출은 10월 1일에 마감되었고, 11월 29일~12월 1일에 4라운드 제출된 수정본을 중심으로 논의하는 4번째 양자 내성 암호 표준화 컨퍼런스가 개최될 예정이다. 해당 컨퍼런스는 제출된 후보 알고리즘에 대해 다양한 관점에서 논의하고 이를 통해 표준화 진행을 위한 피드백을 수용하는 것을 목적으로 하고 있다[4]. NIST는 컨퍼런스를 진행한 이후, 2024년 안에 이용 가능한 양자 내성 암호 표준화 초안을 발표할 계획이라 밝혔다[5]. 양자 내성 암호 표준화 일정에 대한 상세 내용은 [표 3]에서 확인할 수 있다. 현재 NIST에서 선정한 표준화 알고리즘들은 SPHINCS+를 제외하고 모두 격자와 관련된 문제를 기반으로 하고 있다. 특히 전자 서명의 경우 남아있는 후보 알고리즘들도 없는 상황이다. 이에 NIST는 격자 기반이 아닌 다른 문제에 기반하면서도 서명 크기가 작고 속도가 빠른 전자 서명을 요구하고 있다. NIST의 추가 전자 서명 표준화는 2023년 8월 이전에는 시작될 것이라고 예상되고 있다.

표 3 NIST 양자 내성 암호 표준화 상세 일정

일정	내용
2017. 11	알고리즘 제안 마감
2017. 12	Round 1 진출 알고리즘 발표
2018. 04	1차 표준화 컨퍼런스 개최 (제안 알고리즘 소개)
2019. 01	Round 2 진출 알고리즘 발표
2019. 03	Round2 수정본 제안 마감
2019. 08	2차 표준화 컨퍼런스 개최
2020. 07	Round 3 진출 알고리즘 발표
2020. 10	Round3 수정본 제안 마감
2021. 06	3차 표준화 컨퍼런스 개최
2022. 07	최종 선정 알고리즘과 Round 4 진출 알고리즘 발표
2022. 10	Round4 수정본 제안 마감
2022. 11~12	4차 표준화 컨퍼런스 개최 (예정)
2022 ~ 2024	표준화 초안 공개 (예정)

3. 표준암호 알고리즘 정리

1) CRYSTAL-KYBER

NewHope와 같은 Ring-LWE 기반 암호 시스템의 장점은 속도, 키, 암호문 크기의 효율성이며, 단점으로는 효율성과 보안성 사이의 절충안을 민감하게 조정할 수 없어 확장성이 떨어진다. 반면 Frodo와 같은 일반적인 LWE 기반암호 시스템은 확장성은 우수하지만 효율성이 떨어진다. Kyber는 Modul-LWE (Learning With Errors) IND-CCA2 보안을 제공하는 KEM (Key Encapsulation Mechanism) 양자내성암호이다. Kyber가 기반하는 Module-LWE의 경우, 효율성과 보안성 간의 트레이드오프에 대한 절충안을 제공한다. Kyber에서 사용되는 Module-LWE 파라미터의 경우, Ring-LWE와 비교하여 감소된 구조와 우수한 확장성을 가지며, 암호화 성능은 Ring-LWE와 거의 유사하다. 대부분의 격자 기반 암호는 Number Theoretic Transform (NTT)를 활용할 수 있는 파라미터를 선택하는데 Kyber 또한 그러하며 NTT 기반의 곱셈 최적화가 사용된다. NTT 기반의 곱셈은 매우 빠르며, 카라추바와 툼 쿡 기법들과는 다르게 추가적인 메모리를 요구하지 않는다. Kyber는 복호화 실패 확률이 존재하는 격자 기반 암호이다. 복호화 실패가 발생하지 않는 경우, CCA 변환과 보안 주장을 쉽게 만들지만 성능을 감소시킨다. Kyber는 복호화 실패 확률이 존재하지만 극히 낮기 때문에, 이로 인한 보안 공격들에 대해 보안성을 주장함과 동시에 우수한 성능을 제공한다.

2) CRYSTAL-DILITHIUM

Dilithium의 보안성은 격자 안에서 가장 짧은 벡터를 찾기 어렵다는 문제에 기반하고 있다. 또한 Dilithium은 매우 보수적인 보안 강도를 지향하고 있다. 대부분의 격자 기반의 전자서명 알고리즘들은 가우시안 분포상에서의 난수를 추출하지만, 이는 부채널 공격에 취약하며 보안성이 취약한 구현으로 이어질 수 있다. 반면, Dilithium은 Uniform sampling을 기반으로 난수를 생성하고 있음과 동시에, 다른 연산들 또한 Constant 구현에 용이하도록 설계되어 있다. Dilithium 또한 NTT에 적합한 파라미터를 선택함으로써, 곱셈 연산이 최적화된다. Round 2에서의 업데이트 사항인 AES 버전은, 난수를 생성하는데 있어 SHAKE가 아닌 AES를 사용함으로써 연산 효율성을 극대화하고 있다.

3) FALCON

FALCON은 난수를 생성하는데 있어 Gaussian sampling을 사용하지만, 비밀 정보에 대한 누출이 적기 때문에 부채널 공격에 내성을 가진다고 주장하고 있다. FALCON은 전자 서명들 중, 뛰어난 효율성을 제공한다. 같은 보안 강도를 제공하는 격자 기반 전자 서명 알고리즘들과 비교하였을 때, 비슷한 공개키 크기를 가지지만, 서명 크기가 훨씬 짧다. 또한, 고속 Fourier sampling을 사용한 최적화 구현이 가능한데, 이 경우 검증 속도가 5배에서 10배까지 빨라진다. FALCON은 개선된 키 생성 알고리즘을 통해, 30KB 미만의 RAM만이 사용되기

때문에 성능이 제한된 임베디드 장치와의 호환성이 우수하다.

4) SPHINCS+

SPHINCS+는 해시 기반의 전자 서명 알고리즘이며, 매우 보수적인 보안 강도 제공을 지향하고 있다. 내부에서 사용하는 연산이 해시연산이기 때문에 양자내성은 해시의 보안강도에 기반하고 있다. 기존의 해시 기반 전자 서명 알고리즘이 STATE-FUL 형식이었다면 SPHINCS+에서는 STATE-LESS가 가능하게 함으로써 전체 상태를 보존하지 않아도 되는 장점을 가진다. 이를 위해 다중 서명 알고리즘을 최하위 노드에서 적용하였으며 전체적인 구조는 다중 머클트리 형식을 따른다. 다만 다른 양자내성 알고리즘들과 비교하였을 때, 큰 서명 크기와 느린 속도를 가지고 있다는 단점이 있다.

4. Round 4 알고리즘 정리

1) SIKE

SIKE는 SIDH (Supersingular Isogeny Key Encapsulation) 키 교환 프로토콜이며, 타원 곡선들 사이에서의 특정 아이소지니를 찾기 어렵다는 문제에 안전성을 기반한다. SIKE의 장점은 매우 작은 키 크기와 암호문을 제공한다는 점이며, 단점은 암호화 속도가 느리다는 것이다. 하지만 SIKE는 2022년 보안 레벨1에 해당하는 SIKEp434가 약 1시간 안에 일반 컴퓨터 상에서 해킹될 수 있다는 연구 결과가 발표되었다 [11]. 이는 SIKE에 보조점이 존재함과 동시에 비밀 아이소지니가 알려져 있다는 취약점을 활용한 해킹 결과이다. 사실, SIDH의 보조점은, Fault 공격, GPST Adaptive 공격, Torsion Point 공격 등에 활용되던 SIKE의 잠재적인 보안 취약점이었다. 해당 취약점으로 인해 SIKE는 보안 검증의 관점에서 Round 4의 후보 알고리즘으로 분류되었던 것이며, 최근의 해킹 사건으로 인해, 현재 SIKE는 표준화 알고리즘으로 선정되지 못할 것이라는 평가가 이뤄지고 있다.

2) Classic McEliece

Classic McEliece는 Round 4의 코드 기반 암호와 비교하였을 때, 키 크기가 매우 크지만 오랜 역사의 Goppa 코드를 사용함으로써, 매우 보수적인 보안 강도를 지향한다. 키에 대한 압축 메커니즘이 들어가 있지 않기 때문에 키 크기에서는 단점이 존재하지만 동작 성능은 높게 나타나는 장점을 가진다.

3) BIKE

BIKE는 Quasi Cyclic-Moderate Density Parity Check (QC-MDPC) 코드를 사용하는 코드 기반 암호이다. 공개키 행렬이 사용되는 코드 기반 암호에서 첫 번째 행이 전체 행렬을 대표할 수 있는 특징의 QC-MDPC 코드는 키 크기를 줄이는데 효율적이며 BIKE는 높은 성능을 제공한다. 하지만 Decoding 실패 확률이 존재하며, 이로 인한 보안 주장이 완벽하지 않다. 따라서 진행되는 Round 4에서의 철저한 보안성 분석이 요구될 것이다.

4) HQC

HQC는 BIKE와 동일하게 QC-MDPC 코드를 사용하는 코드 기반 암호이다. HQC는 부채널 공격들에 노출된 이력이 있지만[7, 8], 현재 Constant 구현을 통해 부채널 공격에 내성을 가진다고 주장하고 있다. HQC 또한 Decoding 실패 확률이 존재하지만, 이는 실제 공격에는 사용되지 못한다는 점이 강조되고 있다. BIKE와 비교하였을 때, 보수적인 보안 강도를 지향하지만 성능은 떨어진다는 단점을 가진다.

5. 결론

본 고에서는 현재 활발히 진행 중에 있는 NIST 양자내성암호 표준화 공모전 동향에 대해 확인해 보았다. 해당 표준화 공모전의 1차적인 최종 결과로써 표준화 알고리즘이 올해 선정된 상황이다. 다만 암호에 대한 보안 증명이 계속해서 진행 중에 있기 때문에 표준화된 암호에 대한 변동이 추후 충분히 가능할 수도 있다는 특이점이 존재한다. 따라서 암호관련 연구자 및 개발자들은 지속적인 관심을 가지고 해당 양자내성암호 표준화의 변동 사항에 대해 예의주시해야 할 것으로 사료된다.

참고문헌

[1] https://ai.googleblog.com/2020/08/scaling-up-fundamental-quantum.html
[2] https://research.ibm.com/blog/ibm-quantum-roadmap-2025
[3] https://csrc.nist.gov/News/2022/pqc-candidates-to-be-standardized-and-round-4
[4] https://csrc.nist.gov/csrc/media/Projects/post-quantum-cryptography/documents/round-4/history-pqc-round-4-updates.pdf
[5] https://csrc.nist.gov/Projects/post-quantum-cryptography/workshops-and-timeline
[6] W. Castryck, T. Decru. "An efficient key recovery attack on SIDH (preliminary version)." Cryptology ePrint Archive, 2022.
[7] T, Schamberger, J. Renner, G. Sigl, A. Wachter-Zeh, “A power side-channel attack on the CCA2-secure HQC KEM,” Cryptology ePrint Archive, 2020.
[8] C. Hlauschek , N. Lahr, RL, Schroder, “On the timing leakage of the deterministicre-encryption in HQC KEM,” Cryptology ePrint Archive, 2021.

“양자 암호”와 “양자 내성 암호”

1 암호 키(Secret Key)

- 암호 알고리즘과 함께 사용되는 키임
- 기밀성이 유지되어야 하는 모든 암호키(ex.대칭키, 개인키)를 의미함
- 보안매개변수(ex.씨드, 초기값)이 있음

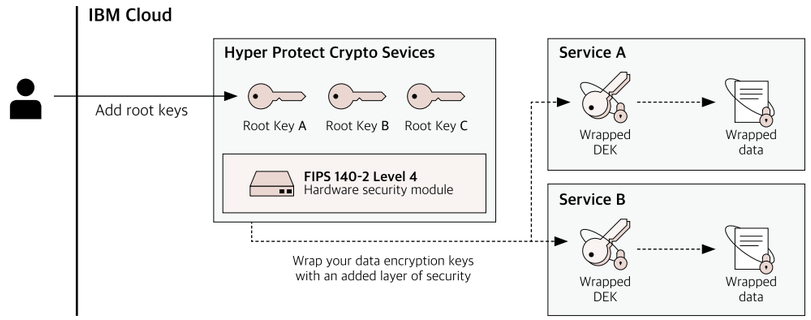
1) 공개키암호(비대칭키)

- 암호화 키와 복호화 키가 서로 다른 암호화 방식임
- 전치암호와 대치 암호의 기법을 사용함
- 인터넷 뱅킹, 전자 주식 거래 등 전자 거래 보안의 핵심이 되는 기술임
- 대표적인 비대칭키: 양자 내성 암호

2) 비공개키암호(대칭키)

- 암호화 키와 복호화 키가 서로 같은 암호화 방식임
- 수학적 계산의 어려움에 기반한 암호기법임
- 전자 서명, 전자 통신, 금융, 의료, 교육 분야에 활용함
- 대표적인 대칭키: 동형암호

암호 키 개념도



출처: International Business Machines Corporation; IBM

2 양자 암호(Quantum Cryptography)

1) 의미

- 양자 역학의 특성을 이용하여 안전하게 정보를 보호함
- 수학적/이론적 방법론 또는 기술적 알고리즘임

2) 등장배경

- 대칭키/비대칭키 암호기법은 일반 컴퓨터의 연산 속도로는 해독할 수 없음
- 그러나 양자컴퓨터의 등장으로 암호해독 가능성이 증명됨
- 비대칭키는 쇼어 알고리즘 기반 양자 컴퓨터의 연산으로 무력화됨
- 대칭키키는 그로버 알고리즘 기반 양자 컴퓨터의 공격으로 암호용량이 커짐

3) 양자 암호 관련 이론연구

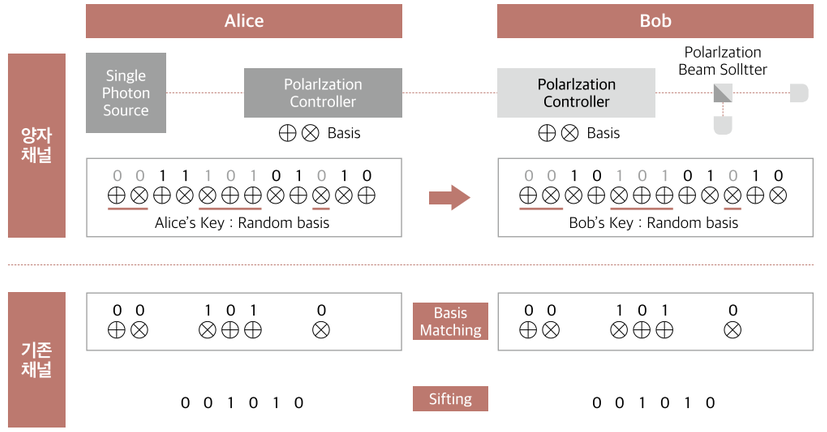
- 새로운 양자 암호 생성

- 대표적인 것은 양자 암호 키 분배(QKD: Quantum Key Distribution)기법임
- 상대방에게 암호를 전달하여 나누어 가질 때 양자 암호 기법을 활용함

- 새로운 양자 암호의 안전성 증명

- 중첩, 얽힘, 복제 불가능성과 같은 물리적 특성으로 안전성을 보장함
- 대표적으로는 1984년 Bennet과 Brasserd가 제안한 BB84기법이 있음

BB84의 암호 키 분배과정



출처: 정보통신기술진흥센터

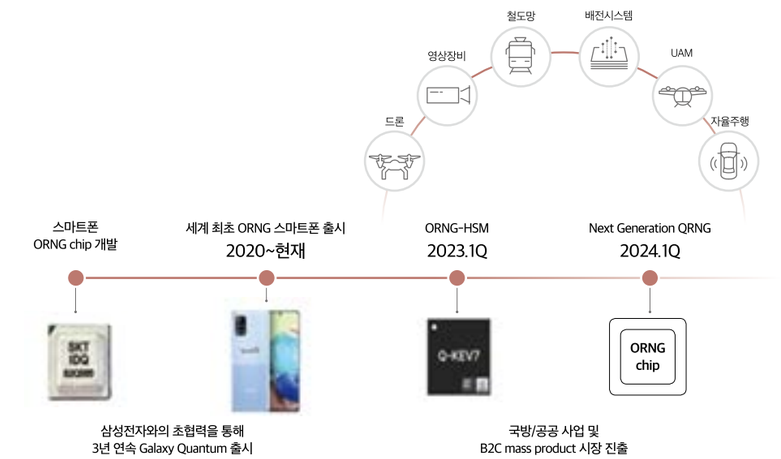
4) 종류

- 이론적 기법 구분: BB84, E91, B92, SARG04 등
- QKD 시스템 구현에 따른 구분: 1-way, 2-way, MDI 등
- 단일 광자의 인코딩 방법에 따른 구분: 편광 부호화, 위상 부호화

5) 양자 암호의 실용 사례

- **SKT의 QRNG 칩 상용화와 양자암호통신망 확대**
- 생체 인증으로 수행하던 보안시스템을 NFC 기능을 활용함
- 통합관제 CCTV 관리자 보안인증 수단으로 채택되어 중요시설 시스템을 보호함

양자 난수 생성(QRNG) 개념도

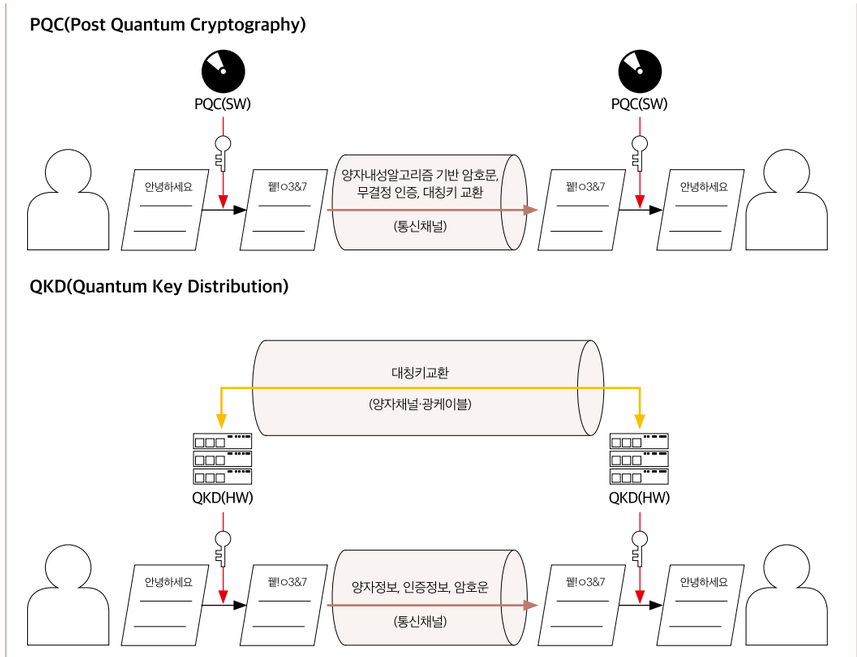


출처: SKT

6) 양자암호통신-양자내성암호 설명도

- 양자암호통신 기술은 별도의 양자키분배 장치와 안정적인 양자키분배 채널이 있고 양자 물리특성을 통해 암호키를 교환하는 기술임
- 반면, 양자 내성 암호는 수학 알고리즘을 통한 암호키 교환, 별도의 대칭키 교환을 위한 광케이블이 불필요하므로 경제성, 안전성을 가짐

PQC-QKD 설명도



출처: LG유플러스

3 양자 내성 암호(PQC)

1) 의미

- 양자 컴퓨터 등장과 그의 위협에 대응하는 비대칭 키 암호 알고리즘임
- 새로운 수학적 난제를 기반으로 양자컴퓨터로도 해독 불가능한 보안성을 갖춤
- 암호키 교환 및 데이터 암·복호화, 무결성 인증 등 다양한 기술을 제공함
- 통신보안, 데이터 보안, 전자상거래 등 소프트웨어 기반 보안에 적용함
- 구축 및 유지 보수 비용 또한 비교적 낮은 장점이 있음

2) 종류

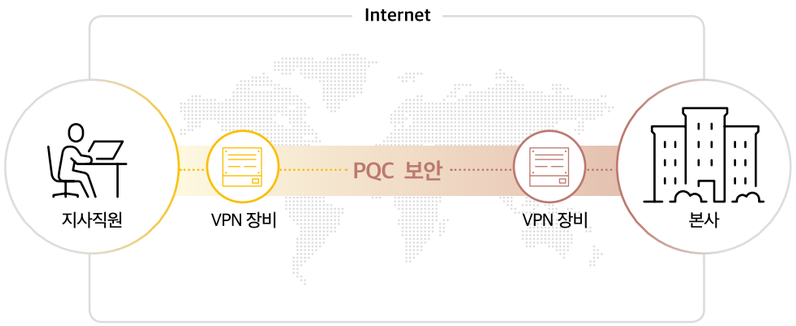
종류	내용
격자 기반 (Lattice-based)	격자(Lattice) 위에서 계산하는 문제의 어려움에 기반하는 암호 시스템
코드 기반 (Code-based)	일반적인 선형 코드(Linear Code)를 디코딩하는 어려움에 기반하는 암호 시스템
다변수 기반 (Multi-variate)	유한체(Finite Field) 위에서 계산하는 다변수함수 문제의 어려움에 기반하는 암호 시스템
해시 기반 (Hash-based)	해시 함수의 안전성을 기반으로 한 전자 서명 시스템
아이소제니 기반 (Isogeny-based)	순서(Order)가 같은 두 타원곡선 사이에 존재하는 아이소제니(Isogeny)를 구현하는 문제의 어려움에 기반을 두는 암호

출처: KISA암호이용활성화사이트

3) 양자 내성 암호의 실용 사례

- SKT, SKB의 글로벌 가상사설망(VPN)에서 PQC 상용화
- PQC 암호화, 키분배 및 전자서명 기술을 적용하여 VPN 강화함
- 미국표준기술연구소(NIST)가 선정한 PQC 후보 중 '크리스털 카이버'와 '크리스털 딜리슘'을 채택함
- 공개암호키와 양자분배키의 조합임
- 양자 암호인 양자암호키분배기(QKD)와 양자난수생성기(QRNG)도 확립함

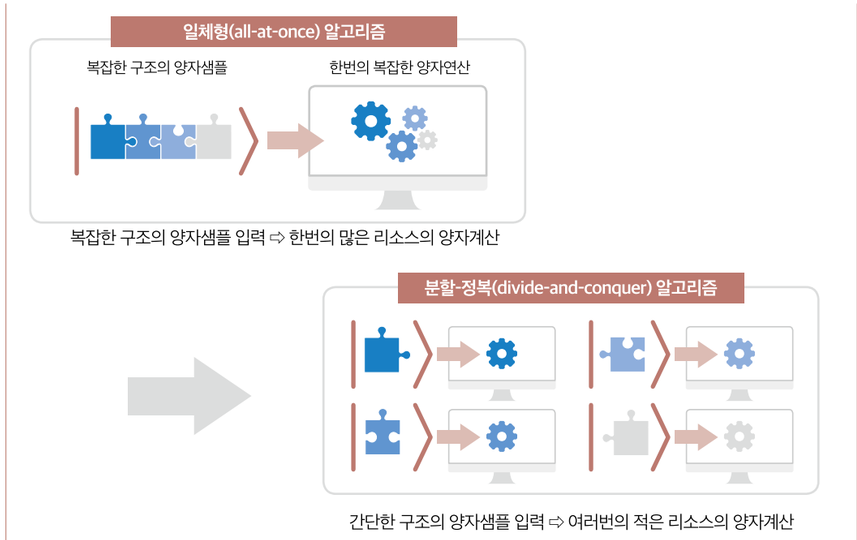
PQC-VPN 개념도



출처: SKT

- 삼성SDS의 기존 암호 네트워크를 양자 내성 암호 체계로 전환
- PQC 암호 알고리즘을 자회사 방화벽 제품에 적용함
- 보안망 위협의 공격을 자동 탐지함
- 네트워크상으로 양자컴퓨터 공격에 취약한 기존 암호 체계를 보완함
- 클라우드 및 제품에 적용된 기존 암호 체계의 양자 내성 암호 지원 예정임

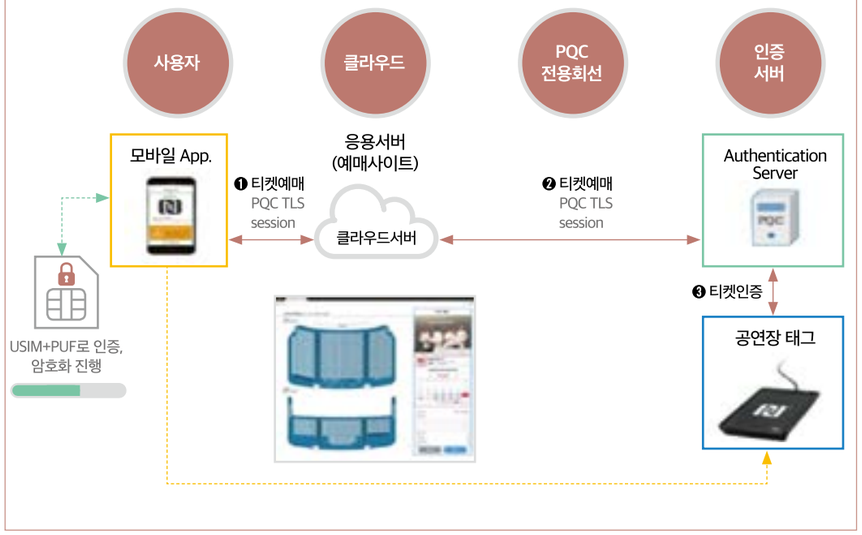
PQC-VPN 개념도



출처: 삼성SDS

- LG유플러스의 해킹 불가능한 양자 내성 암호 보안환경 제공
- 데이터를 송수신할 때 전용회선을 통한 양자 내성 암호 키 교환함
- 네트워크 거리의 제약이 없으며 통신망의 전 구간에 양자 암호 적용함
- 격자 기반 암호의 안전성으로 전용회선 사용이 IOT 환경에 적합함

LG 전용회선 네트워크

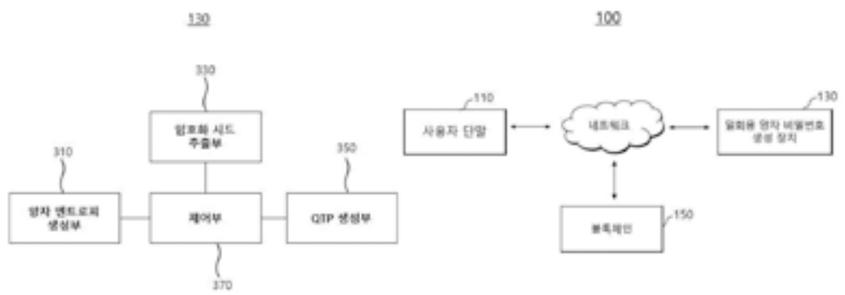


출처: LG

출처

1) TTA 정보통신용어사전
2) KISA암호이용활성화사이트
3) 삼성SDS, 양자내성암호 전환 프로젝트 참여, 전자신문
4) LG유플러스, 세계 최초 양자내성암호 전용회선 서비스 출시, IT 데일리
5) SKT·SKB "글로벌 VPN에서 양자내성암호 상용화", 한국경제
6) ICT Brief, 정보통신기획평가원
7) "막아야 산다" 양자컴 해킹에 맞선 '절대암호' 경쟁 [Digital+]
8) 양자암호통신 기술, ETRI

이건 누가 발견했지?

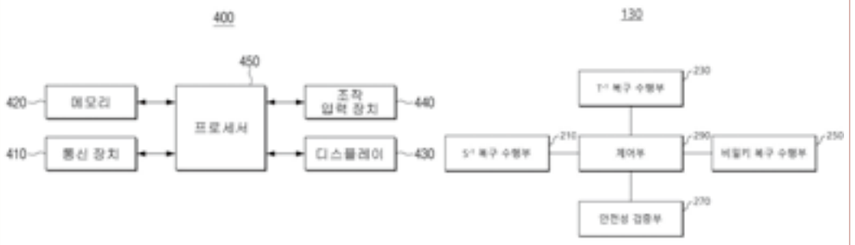


제목	양자 엔트로피 기반 일회용 양자 비밀번호 생성 장치 및 방법
등록번호	KR10-2425077
등록일	2022년 7월 21일
출원인	국민대학교 산학협력단

양자 방사선의 아날로그 잡음원을 발생하여 아날로그 잡음을 제공하는 양자 엔트로피 생성부, 상기 아날로그 잡음에 대한 디지털화를 통해 암호화 시드를 추출하는 암호화 시드 추출부, 및 상기 암호화 시드에 기초하여 일회용 양자 비밀번호(QTP)를 생성하고 상기 일회용 양자 비밀번호(QTP)의 발급 내역을 블록체인 상의 노드에 저장하는 QTP 생성부를 포함

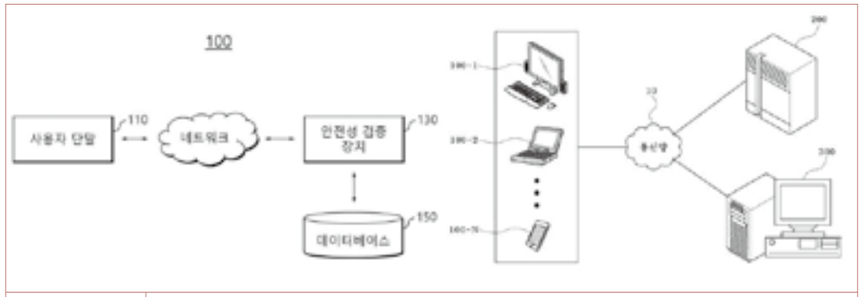
제목	동형암호를 위한 암호화 처리 장치 및 방법
등록번호	KR10-2451633
등록일	2021년 12월 9일
출원인	인하대학교 산학협력단

암호 파라미터를 수신하여 공개키, 비밀키 및 평가키를 생성하는 키 생성기(Key Generation), 다항식을 수신하여 암호화에 적합한 평문으로 부호화하는 부호화기(Encoder)를 포함한 동형암호 장치를 제안



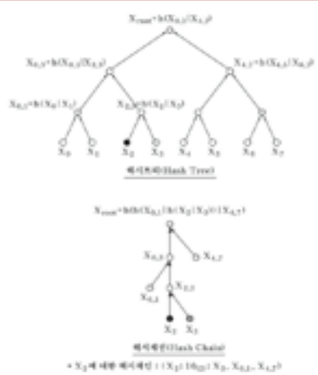
제목	다변수 패킹을 이용하는 연산 장치 및 방법
등록번호	KR10-2339833
등록일	2019년 12월 5일
출원인	주식회사 크립토랩

복수의 메시지를 입력받는 단계, 복수의 메시지를 다변수로 정의되는 다항식으로 인코딩하는 단계, 및 다변수로 정의되는 다항식을 암호화하여 동형 암호문을 생성하는 단계를 포함하는 암호화 방법 개시



제목	다변수 2차 다항식 기반 포스트 양자 서명 스킴의 안전성 검증 장치 및 방법
등록번호	KR10-2067053
등록일	2018년 11월 23일
출원인	국민대학교 산학협력단

서명 값에 관한 제1 부채널 분석을 통해 변환 행렬 S의 역변환 행렬 S-1을 복구를 수행하는 S-1 복구 수행부, 상기 S의 복구가 성공적으로 수행되면 제2 부채널 분석을 통해 변환 행렬 T의 역변환 행렬 T-1의 복구를 수행하는 T-1 복구 수행부 및 상기 T의 복구가 성공적으로 수행되지 않으면 대수적 키 복구 공격을 통해 상기 T와 변환 행렬 F의 복구를 수행하여 상기 S, T 및 F로 구성된 비밀키의 복구를 수행하는 비밀키 복구 수행부를 포함한다. 따라서, 본 발명은 다변수 다항식 기반 서명 스킴에 대해 비침입 공격만을 이용한 비밀키 복구 공격을 통해 안전성을 검증



제목	해시함수 기반의 전자서명 서비스 시스템 및 그 방법
등록번호	KR10-1658501
등록일	2015년 9월 3일
출원인	주식회사 마크애니

전자서명 생성을 필요로 하는 주체가 직접 전자서명을 생성하지 않고 간단하고 안전한 방식으로 알려진 해시함수(Hash Function) 및 해시트리(Hash Tree)를 이용하여 서버(Server) 기반의 전자서명 기반 구조에서 여러 개의 전자문서나 디지털 데이터에 대해 대규모로 동시에 무결성(Integrity)의 전자서명 생성을 안정적으로 수행

양자 내성 암호 분야 특허 동향 및 표준특허 전략

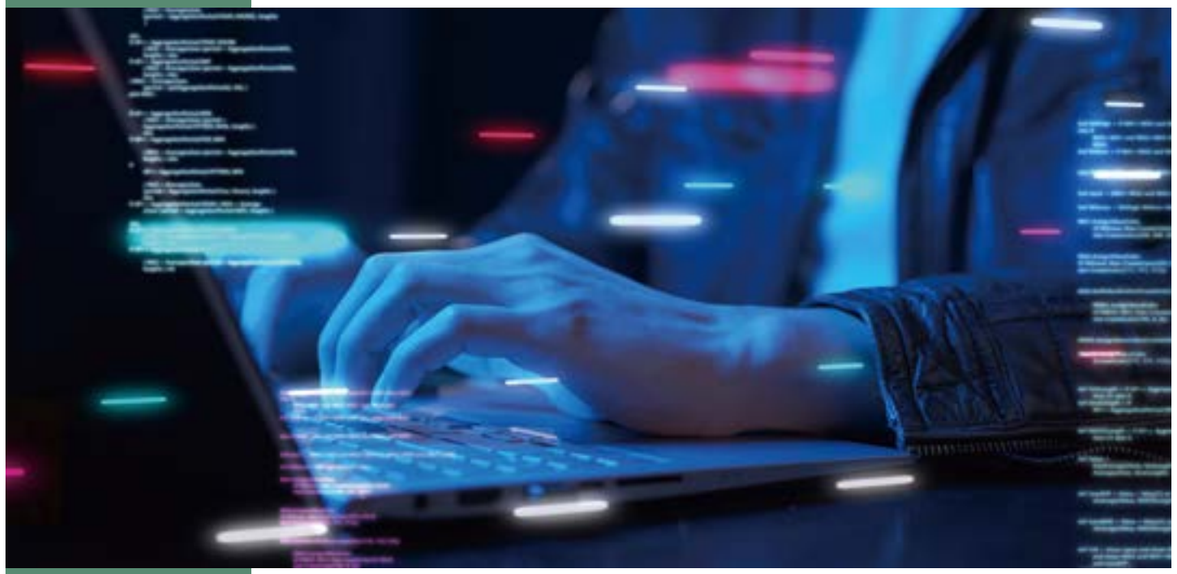
특허법인 지원
백서령 파트너 변리사

① 들어가며

양자 내성 암호(Post-Quantum Cryptography)는 양자컴퓨팅 환경에서 안전하게 암호 기술을 이용할 수 있도록 하는 새로운 암호체계로, 양자컴퓨터의 위협에 대응하여 새로운 수학적 난제를 기반으로 양자컴퓨터로도 해독할 수 없는 보안성을 갖추는 데 초점을 둔다.

특히, 4차 산업혁명 시대가 다가오면서 사회적으로 문제를 일으킬 수 있는 새로운 보안 문제들도 함께 등장하고 있으며, 양자 내성 암호는 이러한 문제들을 해소하고 통신보안, 데이터 보안, 전자상거래 등 응용서비스 보안 등 다양한 산업 분야에 적용할 수 있어, 이를 위한 연구 및 기술개발이 활발히 진행되고 있다.

이에, 본 내용에서는 양자 내성 기술에 대한 특허 동향을 간략히 살펴보고, 표준화 관점에서 양자 내성 기술에 대한 표준특허 창출 전략에 대해 알아보고자 한다.



② 양자 내성 암호 분야 특허 동향

1) 특허 분석 개요

- **(기술의 범위)** 양자 내성 암호의 세부 기술 요소인 암호키 교환 기술, 데이터의 암호화 및 복호화 기술, 무결성 인증 기술을 대상으로 한다.
- **(분석 범위)** Keywert 특허 검색 DB를 이용하여, 한미일, 유럽, 국제(PCT)에 출원/공개(등록)된 특허를 대상으로, 검색구간은 2001.01.01. 이후의 공개 및 등록되어 검색되는 특허로 한정하였다.

일반적으로 특허는 특허출원 후 18개월이 경과 된 때에 출원 관련 정보를 대중에게 공개하도록 하고 있으므로, 2022년 11월까지 공개된 한미일, 유럽, 국제특허를 분석 대상으로 한 본 IPR 분석에서는 미공개 데이터가 존재하는 2021년 5월부터 2022년 11월 사이에 출원된 일부 한미일, 유럽, 국제특허들은 분석 대상에 포함되지 않을 수 있다.

- **(기술 요소 및 키워드)** 암호키 교환 기술, 데이터의 암호화 및 복호화 기술, 무결성 인증 기술의 전략기술 체계 기반으로 구축된 특허 모집단(한국, 미국, 일본, 유럽, PCT)을 활용하여, 양자 내성 암호 분야에 대한 특허 동향을 살펴보고자 한다.

표 1 양자 내성 암호 분야 특허 분석 범위

국가	검색 DB	분석 구간	검색범위
한국	Keywert	2001.01.01. ~ 현재.	특허 공개 및 등록 전체문서
일본			
미국			
유럽			
WO			

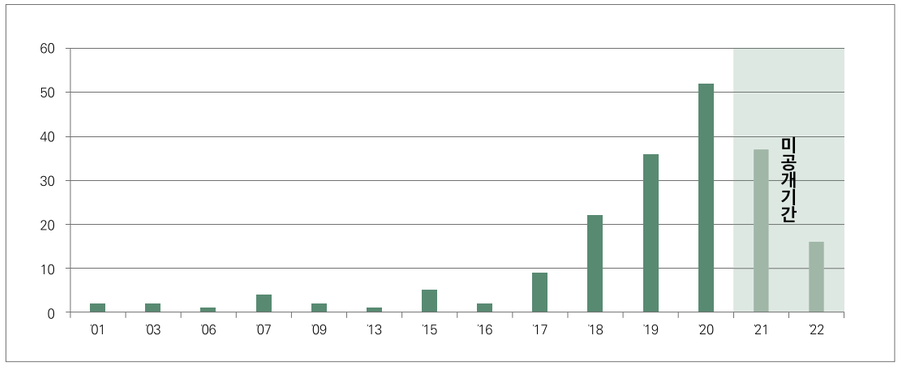
- **(검색식)** 암호키 교환 기술, 데이터의 암호화 및 복호화 기술, 무결성 인증 기술에 포함된 표준화 항목별 핵심 키워드들의 유사/동의어 조합을 통해 특허 검색식을 작성하여 분석을 진행한다.
- **(노이즈 제거)** 검색식을 통해 검색된 특허 모집단에 대하여, 양자 내성 암호 기술 관련성, IPC 분류 확인 및 중복제거를 통해 데이터 필터링을 진행하여 특허 검색 노이즈를 제거하고 유효 특허를 선정하였다.

2) 양자 내성 암호 분야 연도별 동향

양자 내성 암호 분야 분석 대상 표준화 항목 전체 연도별 특허출원 현황을 살펴보면, 2017년부터 증가하여 2018년부터 급격하게 출원 건수가 증가함을 확인할 수 있다.

이는, 2016년 미국 국립표준 기술연구소(NIST)에서 양자 내성 암호 표준 공모를 시작함에 따라, 전 세계적으로 양자 내성 암호에 대한 연구 개발이 진행되면서 관련 특허출원도 증가하는 것으로 판단된다.

그림 1. 연도별 특허출원 동향



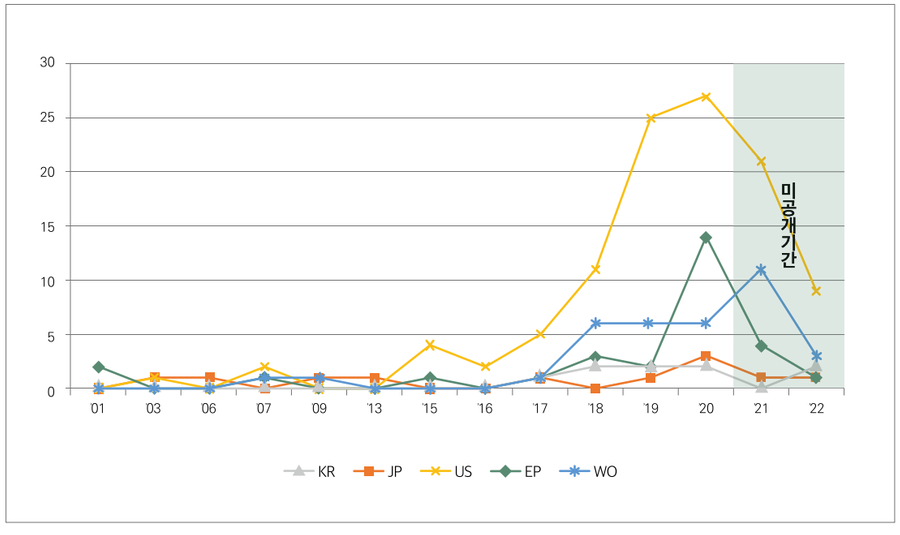
3) 특허 발행국별 연도별 동향

양자 내성 암호 분야 특허 발행국별 연도별 동향을 살펴보면, 미국특허(US) 및 국제특허(PCT)(공개 및 등록 특허 포함)가 각각 107건(56%), 35건(18%)으로 많은 출원량을 보인다.

연도별 특허출원 동향을 살펴보면, 미국(US)의 경우 2017년부터 출원량이 증가하는 모습을 보이고, 한국(KR), 일본(JP), 유럽(EP), 국제(WO) 경우 미국보다 약간 후행하여 2018년도에 증가하는 것을 확인할 수 있다.

이는, 앞서 설명한 바와 같이, 양자 내성 암호 표준 공모를 미국이 시작하여 미국이 연구 개발을 주도적으로 진행하며, 이후 다른 나라들에서 연구를 시작하기 때문으로 사료된다.

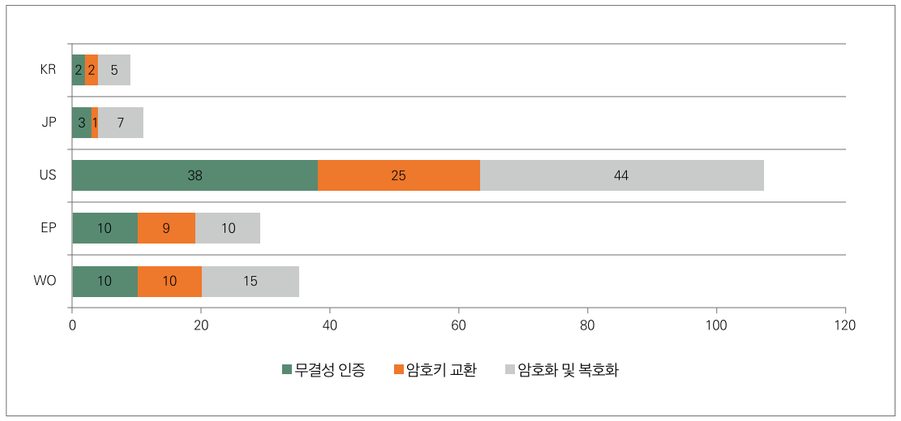
그림 2. 특허 발행국별 연도별 동향



특허 발행국별 연도별 동향의 경우, 2017년 이후에 모든 나라에서 양자 내성 암호 관련 특허출원 건수가 가장 많음을 확인할 수 있으며, 미국 NIST 표준 공모에서 2017년 1라운드가 진행되어 총 69개의 알고리즘이 공개되고, 2019년 2라운드가 진행되어 26개의 알고리즘이 공개되었으며 이에 따른 연구 개발 결과물인 특허출원이 증가한 것으로 사료된다.

또한, 현재 3라운드를 진행하고 있어, 2021년과 2022년에도 특허출원이 증가하였을 것으로 판단되지만, 특허 공개제도에 따라 아직 미공개된 일부 특허출원은 출원량에 포함되지 않았다.

그림 3. 특허 발행국별 요소 기술별 동향



특허발행국별 요소 기술별 동향의 경우, 모든 나라에서 암호화 및 복호화 기술 관련 특허출원 건수가 가장 많고, 무결성 인증과 암호키 교환 기술 관련 특허출원 건수가 그다음으로 많음을 확인할 수 있다.

모든 요소기술에 대하여 미국(US)이 가장 많은 특허출원을 하는 것으로 나타났으며, 글로벌 양자 관련 보안 기술의 시장성이 높은 미국에 특허출원이 집중되는 것으로 사료된다.

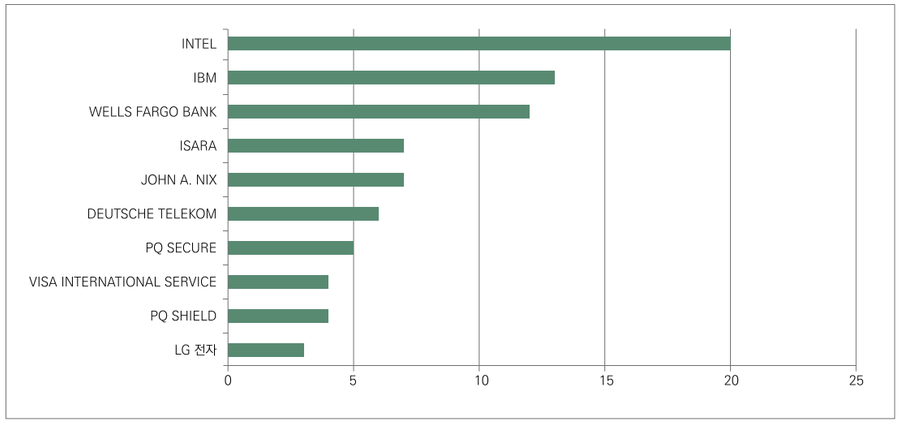
4) 주요 출원인 동향

양자 내성 암호 분야 주요 출원인별 특허 동향을 살펴보면, 글로벌 대기업인 INTEL과 IBM 순으로 많은 특허출원을 하는 것으로 나타났다.

특히, INTEL과 IBM은 미국 NIST와 함께 양자 내성 암호 기술에 대한 표준화 작업을 진행하고 있다. 특히, IBM은 양자 내성 시스템을 탑재한 암호화 기술을 개발하였으며, 양자 내성 시스템인 IBM z16은 데이터 및 시스템 보호를 위한 보안 기본 요소 구성에 대한 접근 방식인 격자 기반의 암호화를 기반으로 한다.

국내 출원인의 경우, LG 전자가 주요 출원인에 위치하는 것을 확인할 수 있으며, LG 전자는 세계 최초로 양자 내성 암호 전용 통신망을 구축한 LG유플러스와 함께 양자 내성 암호 기술을 개발하고 있으며 차량의 사이버보안에 양자 내성 암호 기술을 적용하여 보안을 강화하고 있다.

그림 4: 주요 출원인별 요소 기술별 동향



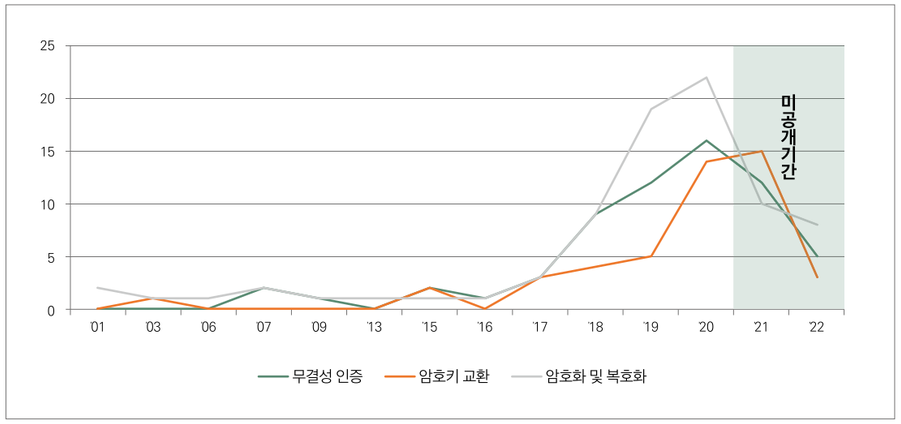
5) 전략기술 체계 요소 기술별 출원 현황

암호키 교환, 암호화 및 복호화, 무결성 인증의 3가지 요소기술 모두에서 2018년에 양자 내성 암호 관련 특허출원 건수가 폭발적으로 증가함을 확인할 수 있다.

요소 기술별 출원 건수의 경우, 암호화 및 복호화 기술에서 81건으로 가장 많은 특허출원이 이루어졌고, 다음으로 63건으로 무결성 인증 기술 순으로 나타났다.

다만, 각 요소기술 모두 2018년 이후 꾸준히 출원 건수가 증가하는바, 암호키 교환, 데이터의 암호화 및 복호화, 무결성 인증과 같은 보안의 핵심 요소와 관련한 보안 서비스 기술에 대한 연구 개발이 전체적으로 진행되고 있음을 확인할 수 있다.

그림 5: 양자 내성 암호 요소 기술별 연도별 동향



3 양자 내성 암호 분야 표준특허 전략

현재 미국 NIST를 중심으로 글로벌 IT 기업들이 양자 내성 암호 기술에 대한 표준화를 진행하고 있으며, 양자 내성 암호의 경우 연구개발(R&D)과 표준개발 상황 모두 초기 단계에 해당하므로 표준화 방향을 분석하여 선출원 지위를 확보하기 위한 출원 전략을 수립하고, 표준에서 정의하는 사양을 포함하는 광의의 용어를 사용하는 권리 범위 설계 전략을 통해 넓은 권리 범위를 확보하는 전략을 수립할 수 있다.

국내의 경우 미국 NIST의 양자 내성 암호 표준 공모에 해외연구팀과 알고리즘을 합동 제안해 2라운드에 진출하였으며, 표준화 초기 단계임을 고려하여, R&D를 진행하면서 해당 결과물을 특허로 출원하고 동시에 표준화 활동을 통해 표준에 반영시키는 전략을 수립할 수 있다.

또한, 국제표준화기구 ISO/IEC에서도 양자 내성 암호 표준화가 진행하고 있는바, R&D에 기반한 표준화 활동을 진행하여 표준화에 선제적으로 대응할 수 있다.

4 마치며

최근에 양자컴퓨팅 기술의 발달로 기존에 있던 대부분의 공개키 암호들이 해독될 수 있다는 사실이 밝혀지면서 양자컴퓨터의 암호화에 대한 위협이 대두되고 있다.

이러한 위협을 해소하는 방안으로 양자 내성 암호 기술에 대한 연구 개발이 진행되고 있으며, 글로벌 시장에서 양자암호 시장의 주도권을 차지하기 위한 경쟁이 활발하게 진행되고 있다.

이러한, 양자 내성 암호는 연구 개발과 표준개발에 있어 초기 단계에 있으므로, 이에 대한 원천기술 및 표준특허를 선점하여 세계 경쟁력을 확보할 수 있을 것으로 판단된다.

따라서, 미래 양자 내성 암호를 기반으로 이루어질 새로운 암호산업의 패러다임의 주도권을 가져오기 위해 산·학·관·연이 협업하여 선제적 기술개발을 진행할 필요가 있다고 여겨진다.

(주)크립토랩

크립토랩

천정희 대표
홍정대 박사

1 (주)크립토랩 소개

데이터를 자유롭게 활용하면서 프라이버시를 함께 보호할 수 있는 시대는 아직 오지 않았다. 국가, 기업, 연구자들은 프라이버시 문제로 AI의 발전에 필요한 데이터를 얻는 것이 어렵다고 하고, 사용자들은 여전히 프라이버시 노출을 우려하는 실정이다.

㈜크립토랩은 세계 최초 동형암호 상용화에 성공하고 양자 내성 암호(Post-Quantum Cryptpgraphy)기술을 보유한 차세대 암호 전문기업으로서, 양자컴퓨팅 공격에도 안전하고 프라이버시 이슈에서 자유로운 AI, Private AI를 실현하기 위해 앞장서고 있다.

㈜크립토랩의 목표는 양자컴퓨터를 방어할 수 있는 4세대 동형암호와 양자 내성 암호 체계를 구현하여 우리의 개인정보 노출을 걱정하지 않고, 데이터를 마음껏 활용하여 편리하고 안전한 세상을 만드는 것이다.

동형암호와 양자 내성 암호에 대한 뛰어난 기술력과 제품화 능력을 바탕으로 2022년 7월, 스톤브릿지벤처스·알토스벤처스·키움벤처스 등 유수의 투자사로부터 210억의 대규모 투자를 유치하였고, 3월에는 IBM의 AI 머신러닝 플랫폼인 'HELayers'에 자사 동형암호 라이브러리 'HEaaN'를 탑재하는 성과를 이루어냈다.

또한, 2019년에는 한국정보통신기술협회(TTA)로부터 크립토랩이 보유한 격자 문제기반 암호 알고리즘인 'RLizard'가 국내 표준으로 인정받았다. 2020년부터 현재까지 LG유플러스와 함께 양자 내성 암호 기술을 공동 기술 개발하여 인프라 구축사업을 추진하고 있으며, 2022년 10월에는 LG전자, LG유플러스와 함께 전장부품 중 차량용 인포테인먼트(IVI; In-Vehicle Infotainment)에 들어가는 양자 내성 암호 기술 개발과 함께 최적화 PQC 사업을 추진하고 있다.

2 (주)크립토랩의 R&D 활동 분야

(1) 동형암호

기존 보안 기술들은 암호화된 자료를 수정하는 등 작업을 수행하려면 암호를 해제해야 하는데 이때 컴퓨터에 열쇠를 함께 보관했어야 했다. 그러다 보니 해커들이 컴퓨터에 침투하여 열쇠를 가로채면 자료를 탈취할 수 있었다. 이러한 문제를 해결하기 위해 동형암호는 열쇠를 컴퓨터에 보관하지 않는다. 컴퓨터에는 오로지 암호화된 자료만 존재한다. 해커는 컴퓨터에 침입하여도 열쇠가 없어 암호화된 자료를 열어볼 수 없는 것이다.

2009년 Gentry의 연구에서 출발한 1세대 동형암호와 동형연산간 발생하는 노이즈를 줄여서 재부팅 횟수를 줄인 2세대 동형암호, 동형곱셈의 연산 시간을 줄인 3세대 동형암호를 거쳐, 부동 소수점 연산(fixed-point arithmetic)과 반올림(rounding) 및 근사계산을 통해 기계학습 등의 응용분야에 상용화가 가능한 4세대 동형암호로 발전해왔다.

2021년 12월 가트너는 2022년 상용화 시기 및 시장 영향력 측면에서 가장 주목해야 할 핵심 기술 5개 중 하나로 동형암호를 선정하였다. 동형암호는 향후 프라이버시 침해 우려 없이 빅데이터를 활용하고자 하는 민간, 공공 분야를 중심으로 빠르게 침투율을 높여갈 것으로 전망된다.

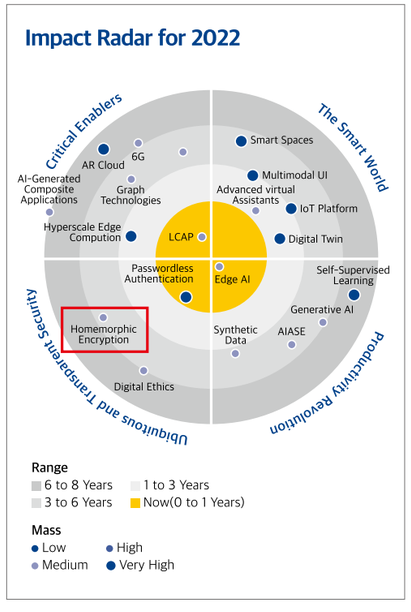
5 Impactful Technologies From the Gartner Emerging Technologies and Trends Impact Radar for 2022

Emerging Tech.		• 총 20개의 유망기술 중 **동형암호는 상용화 시기 및 시장 impact 측면에서 핵심 기술로 선정된 5개 분야 중 하나** - Smart spaces, homomorphic encryption, generative AI, graph technologies and the maeaverse
	Time to market	• **3~6년 내 시장 내 중대한 영향을 미칠 기술로 전망** - 이는 IoT 플랫폼과 Smart Space와 유사한 수준임
	Mass	• **AI 시장 내 Impact 수준은 High로 전망** - 이는 6G와 AR cloud와 유사한 수준임
Sample Vendor		• **크립토랩은 동형암호분야 내 7개 주요 업체 중 하나로 선정됨** - 함께 선정된 업체는 IBM, Microsoft 등이며, US 업체 중 유일하게 선정됨

(2) 양자 내성 암호

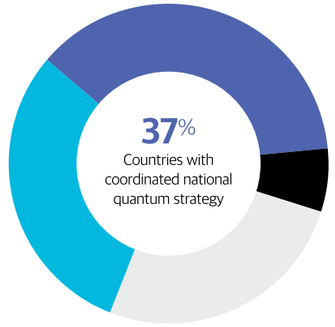
양자컴퓨터는 중첩, 얽힘 등 양자의 고유한 물리학적 특성을 이용하여 다수의 정보를 동시에 처리할 수 있는 새로운 개념의 컴퓨터로서, 현존하는 슈퍼컴퓨터를 모두 합친 것보다 월등히 뛰어난 연산 능력을 발휘할 것이다. 2021년 보스턴컨설팅그룹 보고서에 따르면 양자컴퓨팅은 향후 15~30년 동안 $ 450 ~ 850 billion의 가치를 창출할 것으로 전망하고 있다.

양자컴퓨팅 기술이 태동함에 따라 이면에서는 시스템과 데이터를 보호하고 있는 암호화와 보안을 위협하는 수준 역시 향상되어 기존 암호체계가 파괴될 것으로 전망되고 있다. 전 산업 분야의 기업과 기관은 조직 내 보안 프레임워크에 양자 내성 암호 알고리즘을 채택하여, 양자컴퓨팅으로 무장한 보안 위협에 대응하는 것이 필수로 여겨지고 있다.



양자 내성 암호는 양자컴퓨터로도 풀지 못하도록 만들어진 암호 알고리즘으로 암호화, 키 공유, 전자서명 알고리즘이 개발되고 있다. 양자 내성 암호를 활용하기 위해 미국 NIST(미국립표준기술연구소), 국내 TTA (한국정보통신기술협회) 등에서 표준화를 위한 작업을 수행 중이다.

Figure 1: Quantum-technology R&D policies by country
The proportion of countries with and without coordinated quantum-technology strategies



30.4%
Countries with quantum strategy in development

26.1%
Countries without national strategy, but with significant government or government-endorsed initiatives

6.5%
Countries without significant initiatives but are participants in international quantum partnerships

COORDINATED NATIONAL QUANTUM STRATEGY

Austria	Iran	Slovakia
China	Israel	South Korea
France	Japan	Taiwan
Germany	Netherlands	United Kingdom
Hungary	Russia	United States
India	Singapore	

COORDINATED STRATEGY IN DEVELOPMENT

Canada	South Africa	Thailand

WITHOUT COORDINATED NATIONAL STRATEGY, BUT WITH SIGNIFICANT GOVERNMENT-LED OR ENDORSED INITIATIVES

Australia	New Zealand	Switzerland
Denmark	Norway	United Arab Emirates
Finland	Portugal	
Ireland	Spain	
Italy	Sweden	

WITHOUT COORDINATED SIGNIFICANT INITIATIVES BUT ARE PARTICIOPANTS IN INTERNATIONAL PARTNERSHIPS

Belgium	Estonia	Poland
Bulgaria	Greece	Romania
Croatia	Latvia	Slovenia
Cyprus	Lithuania	Turkey
Czech Republic	Malta	

3 (주)크립토랩의 표준화 활동

(1) 동형암호

크립토랩은 실수연산이 가능한 세계 최초 4세대 동형암호 기술의 원천특허를 보유하고 있으며, 원천특허를 기반으로 다수의 응용 특허를 보유하고 있다. 세계적인 수준의 기술력을 바탕으로 동형암호의 활용 증대와 보급 확대를 위한 글로벌 표준화 활동을 수행하고 있다. 2020년 10월, 마이크로소프트, 인텔, 크립토랩 등 3개 사에 의해 공동으로 ISO 표준으로 제안된 4개의 동형암호 기술이 2021년 10월 만장일치로 New Work Item Proposal에 채택되었습니다. 4개의 동형암호 기술은 각 세대별로, 2세대 BGV, BFV, 3세대 CGGI, 크립토랩 천정희 대표가 개발한 4세대 CKKS이 해당된다. 2022년 현재 Committee Draft 단계이며, 최종 제정단계까지 약 2년의 시간이 소요되어 2024년에는 국제표준으로서 승인 및 제정될 전망이다. 동형암호의 ISO 표준 제정을 통해, 그동안 활용하는데 어려움이 있었던 동형암호의 상용화가 가속화될 것이며, 호환성 증대로 기술 활용도가 증가하여 시장확대를 통한 규모의 경제가 창출되어 글로벌 동형암호 시장이 개화될 것으로 전망된다.

(2) 양자 내성 암호

양자컴퓨팅 공격에 대응하기 위한 양자 내성 암호의 중요성을 높게 인식하고, 2019년 국내 표준 활동을 통해 한국정보통신기술협회(TTA)로부터 양자 내성 암호 알고리즘 'RLizard'가 표준으로 지정되었다. NIST에서 2016년부터 진행하고 있는 양자 내성 암호 표준화 작업에서 1차 표준화 대상으로 선정된 4개의 알고리즘 중 3개가 격자 기반 암호이며, RLizard 역시 격자 기반 암호로서 향후 활용성 역시 기대되고 있다.

4 (주)크립토랩의 주요 성과

크립토랩은 개발한 4세대 동형암호 CKKS를 기반으로 2017년 설립되어 동형암호와 양자 내성 암호의 발전 및 상용화를 위해 다양한 활동을 추진하고 있다.

연도	성과 내용
2022년	• 동형암호 소프트웨어 "헤안 라이브러리" 공개(heaan.it) • IBM 머신러닝 플랫폼에 자사 동형암호 라이브러리 탑재 • 동형암호 기반 챗봇 기술 가능 입증(NACCL 논문) • LG U+와 양자내성암호 기술 협력 계약 체결
2021년	• 동형암호 ISO 신규 표준 아이템(천정희 대표 포함 3인 Editor) • 가트너에서 동형암호 샘플 벤더로 선정 • 세계 최초 동형암호 앱 '코동이(코로나 동선 안심이)' 개발/출시 • CKKS 및 재부팅 특허 미국 등록 • 세계 최초 동형암호 as a Services인 HEaaN Homomorphic Analystics 서비스 출시 : Naver Cloud Platform
2020년	• LG U+와 양자 내성 암호 디지털 인프라 뉴딜사업과제 합동 수행 • 세계 최초 동형암호 기반 데이터 결합 서비스 상용화(국민연금공단, KCB) • 에비드넷과 동형암호 기반 의료데이터 활용 계약 체결
2019년	• 실 데이터에 동형암호 기반 Logistic Regression 학습 가능 입증(AAAI 논문) • 삼성전자 메모리/무전사업부와 공동 기술 개발 • 신용평가기관 KCB(코리아크레딧뷰로) 동형암호 기반 데이터 결합분석 모형 개발 사업 수행 및 금융 샌드박스 승인
2018년	• CKKS 재부팅 및 RNS 기술 개발 • KCB(코리아크레딧뷰로)와 동형암호 데이터 로지스틱 회귀분석 사업 수행
2017년	• 크립토랩 설립

천정희 대표 (주)크립토랩

Question & Answer

Q1 (주)크립토랩이 바라보는 '양자 내성 암호' 분야의 미래 전망은?

양자 내성 암호의 분야 기술의 발전과 표준화 활동들이 활발히 이루어지고 있으며, 이러한 노력들이 응축되어 2024년에는 주요 선진국이 기존 암호 체계에서 양자 내성 암호 체계로 기술 전환을 완료할 것이며, 주요 국가의 정부 뿐만 아니라 글로벌 기업들의 수요 역시 증가할 것으로 전망된다.

2021년 미 국가안보국(NSA)은 양자암호통신(양자키분배, QKD)을 공공서비스에 사용하지 말 것을 권장했다. 현재 NSA와 미 국립표준기술연구소(NIST) 등 미국 정부는 2024년까지 양자 내성 암호 기술 표준화 및 검증 작업 완료를 목표로 기존 공개키 암호기술 전환 작업을 진행하고 있다. 영국에서도 국립사이버안보센터(NSCS)를 통해 정부와 국방 분야의 앱에 QKD 사용을 보증하지 않는다고 밝혔다. QKD 방식이 보증받지 못함에 따라 양자 내성 암호 방식이 더욱 신뢰성을 검증받고 활용성이 확장될 것으로 전망된다.

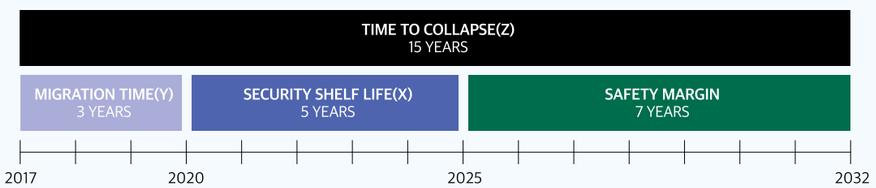
국내에서는 산·학·관·연 협업 기반의 양자 내성 암호 기술 개발 및 국내 알고리즘 공모를 위한 양자내성암호연구단을 구성하여, 공개키 암호, 키 설정, 전자서명을 대상으로 양자 내성 암호 국가공모전이 추진되고 있다. 국내에서의 암호 체계의 변화에 맞추어 국내 기관과 기업들의 양자 내성 암호에 대한 수요 역시 증가할 것으로 전망된다.

Q2 양자 내성 암호 분야 표준화를 시작하게 된 계기는?

양자컴퓨팅 시대는 빠르게 도래할 것이며, 이에 대응할 수 있는 암호 기술을 개발하고 널리 보급/확대하는 것이 암호 연구자 및 암호 전문기업의 대표로서 수행해야 하는 역할이라고 생각하였으며, 양자 내성 암호의 활용에 있어 첫 걸음이 표준화라고 생각한다.
양자컴퓨팅 공격에도 깨지지 않는 양자 내성 암호의 기준을 수립하는데 일조하고자 표준화 작업에 참여하게 되었다.

Q3 양자 내성 암호 분야에서 주목해야 할 부분은?

현재 양자 내성 암호 분야의 연구 및 기술개발은 주로 양자컴퓨팅 공격으로 깨지냐, 안깨지냐 즉, 암호 알고리즘의 보안성과 안정성에 대하여 주로 다루고 있다. 암호 알고리즘의 보안성과 안정성이 중요한 것은 맞지만 기존 암호체계인 공개키 암호 인프라가 양자 내성 암호로 전환할 때에 어떻게 전환되어야하는지, 전환시점은 언제인지 등에 대하여 다루어져야 한다.



양자 내성 암호 체계로의 전환 효과는 양자컴퓨팅 시대가 돌입하고 난 이후 확인할 수 있지만, 전환에 대한 대비는 사전에 이루어지기 때문에, 전환 이전에 고려해야 할 사항(암호의 수준, 비용, 기대효과 등) 들에 대해서도 충분히 연구되고, 암호 활용처에서는 체계적으로 전환 계획이 수립되어야 한다.

Q4 앞으로 도전하고자 하는 과제는?

크립토랩에서는 양자 내성 암호팀을 별도로 구성하여 양자 내성 암호 기술 개발과 사업화를 위한 사업을 추진하고 있다. 양자 내성 암호 기술개발에 대하여 기존의 RLizard 이외에 키교환과 전자서명에 대한 알고리즘을 추가로 개발함으로써 양자 내성 암호 기술 개발의 범주와 수준을 높일 계획이다. 이를 위해 양자 내성 암호 분야에서 유명한 해외 대학 교수님과도 협력하고 있다.
또한, 국내와 해외의 표준화 활동에 적극적으로 참여하고, 기존 표준화 활동에 박차를 가함으로써 양자 내성 암호 기술의 시장 적합성과 경쟁력을 향상시키고, 기술개발의 기준을 확립하고자 한다. 기술개발과 표준화 노력을 통해 양자 내성 암호 기술의 제품화 및 상용화를 통해 양자 내성 암호 체계와 기술 자체에 수요가 있는 정부, 기업, 개인이 양자 내성 암호를 효과적으로 쉽게 사용할 수 있도록 하는 것이 주요 과제이다.

Q5 '양자 내성 암호'기술 분야에서 바라는 정부의 요구사항은?

양자 내성 암호와 더불어 암호 분야는 지식재산과 아이디어보다 눈에 보이는 하드웨어가 산업을 주도하다 보니, 가치를 산정하거나 평가하여 지원하는 체계는 미흡한 것으로 보인다. 그러나 세상에서 직접적으로 활용되고 더 큰 가치를 주는 것은 아이디어와 소프트웨어라고 생각한다. 암호 알고리즘을 개발하고 탑재하여 소프트웨어화하는 것 역시 중요하기 때문에 암호 분야에 대한 가치가 온전히 평가되어 지원정책이 추진되었으면 좋겠다.
이와 더불어 단순히 소프트웨어 개발 인력만이 중요한 것이 아니라 알고리즘에 대하여 심도 깊게 연구할 수 있는 인력과 자원이 필요하다. 데이터 산업 육성 정책이 활발히 이루어지고 있는 만큼 데이터 보호 관점에서 암호 알고리즘을 연구하고 개발하는 인력 양성과 인력에 대한 지원을 통해 양자컴퓨팅 시대를 함께 대비할 수 있는 전문가가 많아져 함께 일하기를 기대한다.

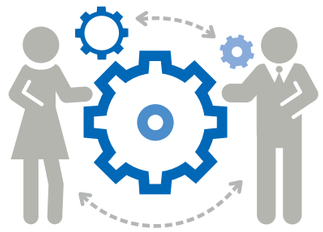
표준특허 관련 주요 행사

1 추진 사항

2022년 표준특허 인식확산 교육 개최

지난 11월 23일 표준특허에 관심 있는 포럼 및 협회 회원사를 대상으로 표준특허 인식 확대 및 중요성 제고를 위해 교육을 개최했다. 교육은 위플레이스 강남점(강남구 강남대로340, 경원빌딩 3층)에서 진행되었으며 지식재산권, 표준특허의 이해 및 실무 활용 방안을 내용으로 교육을 구성하였다. 세부 사항으로 특허, 상표권 및 표준특허의 개념 및 활용전략을 주제로 교육을 진행하였다.

2 예정 사항



(ICAPQC 2023)International Conference on Advances in Post-Quantum Cryptography

- **일 시** : 2023년 5월 4일 ~ 2023년 5월 5일
- **주 최** : International Conference on Advances in Post-Quantum Cryptography
- **내 용** : Post-quantum cryptography, Quantum computing
  ※ 자세한 내용은 http://waset.org 참고

2023년 표준특허 전략지원 사업 대상 과제 모집

- **일 정** : 2022년 12월 ~ 2023년 1월 中
  * 내부사정에 의해 사업공고 일정은 변경될 수 있음
- **주 최** : 한국특허전략개발원 표준특허센터
- **대 상** : 국제표준 관련 연구개발, 표준화 활동을 수행하고 있는 중소·중견기업, 대학 ·공공연 및 협회
- **지원내용** : 국제표준화 및 표준특허 확보를 위한 R&D 방향, 표준특허 확보를 위한 특허 설계·출원·보정 전략, 보유특허 및 표준화 동향을 반영한 표준안 보완 전략 등 제공
  ※ 자세한 내용은 추후 http://biz.kista.re.kr/epcenter 참고

2023 찾아가는 맞춤형 표준특허 교육대상 모집

무료

표준특허센터에서는 표준특허 교육을 희망하는
다수의 인원이 소속된 기업 또는 기관에 대하여 원하는 컨텐츠 및
시간·장소에 맞춰 **무료로 표준특허 교육을 제공**하고 있습니다.

대 상 표준특허 교육을 희망하는 산·학·연 누구나
모집기간 상시(~2023.11)
비 용 전액무료
신청방법 표준특허포털(http://biz.kista.re.kr/epcenter/eduReq.do)에서 온라인 신청

진행과정

교육신청 접수	포털사이트를 통해 교육 수요 접수(상시)
교육생 자가진단	표준특허 인식수준 및 수요조사
교육프로그램구성	진단결과 기반 맞춤형 프로그램 협의
교육개최	방문교육 진행

기 타
- 교육 수료 후, 수료증 발급 가능
- 문의처: 표준특허센터 복영건 연구원 (02-3475-8573, epcenter@kista.re.kr)

SEP Inside
Standard Essential Patent

표준특허 전문지 Vol.36

SEP Inside 편집위원

편집위원장
신원혜 특허청 산업재산창출전략팀장

편집위원
김 호 영 특허청 산업재산창출전략팀
이 기 민 특허청 산업재산창출전략팀
김 융 한국특허전략개발원 표준특허센터
이 준 우 한국특허전략개발원 표준특허센터
이 수 일 한국특허전략개발원 표준특허센터
윤 순 영 한국특허전략개발원 표준특허센터
김 아 란 한국특허전략개발원 표준특허센터
이 다 영 한국특허전략개발원 표준특허센터
이 예 진 한국특허전략개발원 표준특허센터

SEP Inside Vol.36

발 행
특허청 산업재산창출전략팀
한국특허전략개발원 표준특허센터

발행일
2022년 12월 1일

발행인
이 재 우 한국특허전략개발원장

발행처
한국특허전략개발원
[본원] 대전광역시 중구 대종로 540 유안타증권빌딩 14층, 15층 (34831)
[분원] 서울시 강남구 테헤란로 131 한국지식재산센터 8층 (06133)
홈페이지 : http://www.kista.re.kr
http://biz.kista.re.kr/epcenter