정 보 보 호 학 회 지
제 33 권 제3호, 2023. 6

양자내성암호 국가공모전

이 나 리*, 정 경 철**, 지 성 택***, 한 대 완****

요 약

1990년대에 P. Shor가 소개한 양자 알고리즘에 의해 양자컴퓨팅을 사용하여 다항식 시간 내에 인수분해나 이산대수 문제를 해결할 수 있다는 것이 알려졌다. 양자컴퓨터의 실용화가 기존 공개키 암호에 심각한 위협이 되는 것이다. 이에 대한 대응으로 많은 국가들이 양자내성암호 개발 및 표준화에 힘쓰고 있으며, 대표적으로 미국의 국립표준기술연구소(NIST)가 2017년에 양자내성암호 표준화 공모사업을 시작하였다. 국내에서도 양자내성암호 분야의 활성화 및 자체 기술력 확보를 위해 노력하고 있다. 그 일환으로 국가보안기술연구소가 국가정보원의 후원으로 2021년에 발족한 양자내성암호연구단은 현재 '양자내성암호 국가공모전'을 진행하며 양자내성암호 개발에 힘쓰고 있다. 이 논문에서는 1라운드가 진행 중인 양자내성암호 국가공모전의 추진 배경, 취지 및 진행 상황을 소개하고자 한다.

Ⅰ. 서 론

1981년 물리학자 Richard Feynman에 의해 처음 소개된 양자컴퓨팅은 1985년 David Deutsch가 제시한 양자 알고리즘에 의해 더욱 구체화되었다. 이후 Shor 알고리즘[1], Grover 알고리즘[2]과 같이 암호분석에 활용이 가능한 양자 알고리즘이 제시되며 양자컴퓨터의 개발 시기가 큰 관심을 받기 시작하였다. 최근에는 IBM, 구글, 마이크로소프트, 인텔과 같은 글로벌 IT 기업들이 공격적인 투자를 하면서 양자 컴퓨터 개발에 속도를 내고 있다.

이러한 양자컴퓨팅 기술의 발전은 기존 공개키 암호체계에 대한 위협으로 이어진다. Shor 알고리즘은 인수분해나 이산대수 문제를 다항식 시간 내에 해결한다고 알려져 있으며, Grover 알고리즘은 비밀키암호의 키 탐색 전수조사의 복잡도를 $O(N)$에서 $O(\sqrt{N})$으로 낮추는 것으로 알려져 있다. 각 알고리즘이 현 암호체계의 보안 강도에 미치는 영향은 [표 1]에서 구체적으로 확인할 수 있다.

공개키 암호체계가 양자컴퓨터에 대하여 안전성을 보장받기 위해서는 기존의 공개키 암호를 양자내성암호(Post Quantum Cryptography, 이하 PQC)로 전환할 필요가 있다. 이에 따라 선진국을 중심으로 PQC로의 전환 계획이 수립되고 있으며, 한국 또한 PQC로의 전환에 대한 논의가 진행되고 있다. 국내에서는 NIST와 같은 표준화 기관이 주관하는 암호 공모사업은 없으나 양자내성암호연구단(이하 KpqC 연구단)이 2021년부터 양자내성암호 국가공모전을 진행하는 등 주도적으로 국내 PQC 관련 사업을 운영하고 있다.

본 논문의 2장에서는 양자컴퓨터의 최근 개발 동향과 이에 대한 국외 대응 동향을 살펴보고, 3장에서는 양자내성암호 국가공모전의 개최 취지, 진행 상황 및 추후 계획을 소개하고자 한다.

〔표 1〕 양자 알고리즘 적용에 따른 암호체계의 보안강도

타입	알고리즘	보안 강도(bit)		양자 공격
		고전	양자	
공개키 암호	RSA-2048	112	다항식 시간	Shor 알고리즘
	RSA-3072	128		
	ECC-256	128		
	ECC-521	256		
비밀키 암호	AES-128	128	64	Grover 알고리즘
	AES-256	256	128	

* ETRI 부설연구소 (선임연구원, narilee@nsr.re.kr)
** ETRI 부설연구소 (실장, jeongkc@nsr.re.kr)
*** ETRI 부설연구소 (책임연구원, chee@nsr.re.kr)
**** ETRI 부설연구소 (센터장, dwh@nsr.re.kr)

Ⅱ. 양자컴퓨터 개발 상황 및 국외 대응 동향

2.1. 양자컴퓨터 개발 상황

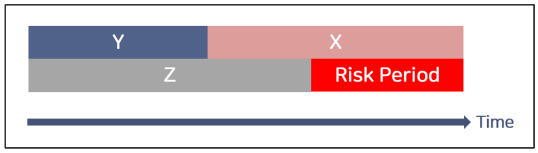
구글은 2018년도에 미국 물리학회에서 72 큐빗 양자 프로세서 Bristlecone을 소개하고, 2019년도에 Nature를 통해 53 큐빗 양자 프로세서 Sycamore를 공개하였다. 구글은 오류율이 높아 양자 우월성을 달성하지 못한 Bristlecone과 달리 Sycamore는 오류율을 대폭 낮추며 양자 우월성을 달성하였다고 주장하였다. 그러나 이 결과에 대해 IBM은 그 우수성은 인정하지만 양자 우위에 도달한 것은 아니라고 주장하였다. 두 기업의 이러한 설전에도 불구하고 구글의 양자 기술 개발은 양자 컴퓨터의 실용화에 한발 다가간 것으로 해석될 수 있다. 구글은 2021년도에 Quantum AI Campus를 설립하여 지속적으로 양자컴퓨터의 설계·개발을 진행하고 있다.

IBM은 2020년도에 65 큐빗 양자 프로세서 Hummingbird를 공개하였고, 이와 동시에 1,000큐빗 이상의 양자 프로세서 개발 계획이 포함된 로드맵을 발표하였다. 2021년도에는 127 큐빗 양자 프로세서 Eagle을 선보였는데, 이는 100 큐빗을 넘어서는 최초의 결과였다. 2022년도에는 433 큐빗 양자 프로세서 Osprey를 출시하였으며, 2023년도에는 1,121 큐빗의 양자 프로세서 Condor를 출시할 예정이다. 1,000 큐빗 이상의 양자 프로세서의 경우 고성능 냉각장치가 필요하다. 이에 IBM은 1,000 큐빗이 아닌 100만 큐빗 이상을 함께 염두에 두고 슈퍼 냉각 장치(Goldeneye)를 직접 개발하고 있다. 이러한 기술들을 기반으로 IBM은 향후 10년 이내에 100만 큐빗의 대규모 양자 컴퓨터 개발을 목표로 하고 있다.

이 외에도 클라우드 양자컴퓨팅 서비스로 아마존은 2019년부터 Amazon Braket을, 마이크로소프트는 2022년부터 Azure Quantum을 운영하고 있다.

2.2. 양자컴퓨터 위협에 대한 국외 대응 동향

이러한 양자컴퓨터 개발 기술의 발전에도 불구하고 그 실용화 시기를 예측하기는 매우 어려운 일이다. 캐나다 Waterloo 대학의 Mosca 교수는 2013년 유럽 ETSI Quantum Cryptography Workshop에서 양자컴퓨터 실용화에 대비하기 위한 준비기간 산정의 근거로 [그림 1]을 제시하였다[3].



〔그림 1〕 Mosca의 부등식

- X : 보호하려는 대상의 보안 유지가 필요한 기간
- Y : PQC 암호로의 전환에 필요한 기간
- Z : 양자컴퓨터가 현실화되는데 필요한 기간

이때, 각 경우에 대한 안전성은 다음과 같다.

1) $X+Y>Z$: 양자컴퓨터를 이용한 공격 가능
2) $Y>Z$: 가능한 빨리 전환해도 안전성 보장 불가
3) $X+Y<Z$: 양자내성암호로의 전환을 통한 양자 위협 대비 가능

Mosca의 부등식에서는 X의 역할이 중요하다. 이는 국가 간 외교 기밀문서 등 내용에 따라 오랜 기간 기밀이 유지되어야 하는 데이터가 존재하기 때문이다. 이런 경우에는 “Harvest now, decrypt later” 라고 불리는, 사전에 암호문을 수집해놓고 양자컴퓨터가 실용화된 이후에 해독하여 정보를 취득하는 방법이 가능하다. 따라서 [그림 1]의 Mosca 부등식은 각 데이터의 특징에 따라 그 의미를 달리 해석하는 것이 적절하다 하겠다. 그러나 일반적인 경우에는 Y와 Z로 표현되는 PQC 알고리즘의 개발 시기와 양자컴퓨터 실용화 시기의 문제로 귀결될 것으로 예상된다.

2.2.1. NIST의 대응 동향

미국의 국가안보국(NSA)은 2015년에 Suite B를 PQC로 대체할 계획에 대하여 발표하였다. Suite B는 NSA에서 기밀정보보호를 위하여 미국 정부 기관의 요구 사항을 충족하는 암호알고리즘 집합을 대표하는 이름이다. 이후 2017년에 NIST는 전세계를 대상으로 PQC 표준화 공모사업을 시작하였다. 2022년도에는 표준화 알고리즘 4종을 선정했고, 동시에 공모전 4라운드 및 전자서명 추가 공모의 시작을 알렸다[표 2].

당해 미국의 백악관은 국가안보공문에서 구체적인 양자내성암호 전환 전략을 발표하였고[4], NSA는 CRYSTALS-Kyber와 CRYSTALS-Dilithium이 포함된 미국의 상업용 국가 안보 알고리즘 CNSA 2.0 버전을 발표하면서 2030년까지 미 정부의 주요 시스템

〔표 2〕 NIST PQC 표준화 추진 현황 및 계획

시기	내용	비고
'16.2.24.	표준화 개시 공고	
'17.11.30.	알고리즘 공모 마감	82종 제출
'17.12.22.	1라운드 선정 알고리즘 발표	69종 선정
'19.1.30.	2라운드 선정 알고리즘 발표	26종 선정
'20.7.23.	3라운드 선정 알고리즘 발표	최종 7종, 대안 8종 선정
'22.7.6.	표준화 대상 알고리즘 발표 - PKE/KEM ・CRYSTALS-Kyber - 전자서명 ・CRYSTALS-Dilithium ・Falcon ・SPHINCS+	표준화 4종 선정
	4라운드 선정 알고리즘 발표	4라운드 4종 선정
'22.7.6.-'23.6.1.	전자서명 알고리즘 추가 공모	

〔표 3〕 CNSA 1.0과 CNSA 2.0 알고리즘 비교

CNSA 1.0		CNSA 2.0
・AES ・ECDH ・ECDSA ・SHA-384 ・DH 키 교환 ・RSA 키 설정 ・RSA 전자서명	⇒	・AES ・CRYSTALS-Kyber ・CRYSTALS-Dilithium ・SHA-384 / SHA-512 ・LMS ・XMSS

내 PQC 전환 완료를 목표로 하고 있다고 밝혔다. CNSA 2.0은 기존에 CNSSP (The Committee on National Security Systems Policy) 15, Annex B에 작성되어 있던 CNSA 1.0 알고리즘에 대한 업데이트 버전으로 세부 알고리즘 변경사항은 [표 3]과 같다[5].

2.2.2. 국제 표준화 동향

현재 국제 표준화 기구(ISO)에 표준화로 제안이 된 알고리즘으로는 해시 기반 전자서명 알고리즘 중 XMSS, XMSS-MT, LMS, HSS 등이 있으며, 이들은 현재 위원회 단계 연장(2nd Committee Draft) 과정 중에 있다. KEM 알고리즘으로는 FrodoKEM, Classic McEliece, CRYSTALS-Kyber가 있으며 현재 예비단계(Preliminary Work Item)까지 승인되었다. FrodoKEM은 독일의 연방정보기술보안청(BSI)이 제안하였고, Classic McEliece는 개발자들이 제안하였다.

2.2.3. 기타 동향

중국도 2018년에 자국 내에서 [표 4]와 같은 일정으로 암호공모전을 시행하여 2020년에 2라운드를 마치며 최종 알고리즘으로 1/2/3위를 구분하여 선정하였다. NIST의 PQC 공모전과 달리 중국은 PQC와 함께 블록암호도 공모하였고 NIST가 3라운드 내지는 4라운드를 진행한 후에 최종 알고리즘을 선정하는 것과 달리 중국은 2라운드 진행 후 1/2/3위의 알고리즘을 선정하였다.

유럽에서는 독일의 BSI가 자국 내 PQC 알고리즘으로 Classic McEliece, FrodoKEM, XMSS, LMS, HSS, XMSSMT를 사용할 것을 권장하고 있다[6]. 네덜란드의 국가통신보안국(NLNCSA)은 FrodoKEM과 Classic McEliece를 사용할 것을 권장하고 있다[7]. 프랑스의 국가정보시스템보안청(ANSSI)은 FrodoKEM, CRYSTALS-Kyber, CRYSTALS-Dilithium, Falcon을 추천하고 있다. 프랑스의 경우에는 2021년에 양자컴퓨터 관련 분야에 10억 유로 이상을 투자할 것을 발표하였고, 2022년에 ANSSI가 양자내성암호로의 3단계 전환 로드맵을 제시하였다. ANSSI는 PQC 전환의 당위성, 하이브리드 전환의 필요성, 새로운 암호 적용의 적합성과 용이성 등의 이슈에 대해 독일의 BSI와 비슷한 관점을 가지고 있음을 밝혔다[8].

〔표 4〕 중국 암호 공모전

시기	내용	비고
'18.6.	공모전 공지	
'19.2.28.	알고리즘 제출 마감	
'19.3.15.	1라운드 알고리즘 발표	・블록암호: 22개 ・공개키 : 38개
'19.9.27.	2라운드 알고리즘 발표	・블록암호: 10개 ・공개키 : 14개
'20.1.2.	최종 결과 발표	・2라운드 알고리즘을 1/2/3위로 구분

Ⅲ. 양자내성암호 국가공모전

양자내성암호 국가공모전은 KpqC 연구단에서 주최하고 있으며, KpqC 연구단은 국가보안기술연구소가 국가정보원의 후원으로 2021년에 결성하여 다음의 목적으로 운영되고 있다.

- 국내 PQC 기술력 제고 및 저변 확대
- PQC 분야의 인력양성
- 산·학·연·관의 협업으로 선제적 기술 개발
- 양자내성암호 국가공모전 개최

KpqC 연구단의 핵심 추진사항 중 하나가 양자내성암호 국가공모전 개최이다. 앞장에서 살펴보았듯이 여러 기업이 양자컴퓨터 개발에 박차를 가하는 것과 동시에 세계 주요 국가들은 양자컴퓨팅 위협에 대응하기 위해 발 빠르게 움직이고 있다. 국내에서도 한국형 양자내성암호 기술을 확보할 필요가 있으며 PQC와 관련하여 NIST의 정책과는 별도로 국내 상황에 맞는 정책을 추진할 필요가 있다. KpqC 연구단은 이러한 상황에 맞춰 국내 PQC 기술력 제고를 위해 2021년에 양자내성암호 국가공모전을 시작하였다.

다음 소절에서는 지금까지 양자내성암호 국가공모전이 진행된 상황을 소개하고 각 과정에서의 주요 고려사항과 추후 계획을 살펴보도록 하겠다.

3.1. 공모전 0라운드

연구단은 국내 PQC 분야의 저변이 넓지 않은 점을 고려하여 ‘공모전 0라운드’라는 개념을 도입하였다. 공모전 참가자들은 0라운드에서 알고리즘 설계서를 간소화한 개발계획서를 2022년 2월 18일까지 제출하고 알고리즘을 개발할 수 있는 약 9개월의 기간을 부여받았다. 개발계획서에는 구체적인 알고리즘 대신 알고리즘 기능, 기반 문제, 설계방식 및 특징, 장점, 목표 성능, 개발 계획 등을 간략히 기술하도록 하였다. 공모전 참여자는 복수의 개발계획서를 제출하는 것이 가능하였으며 개발자의 연구 결과 중 국내외 저널/학회에 게재된 논문이나 기존에 발표된 연구 결과도 제출할 수 있도록 하였다[1].

0라운드 알고리즘은 평가위원단이 다음과 같은 평가 기준으로 심사한 결과 총 18종이 채택되었다.

〔표 5〕 0라운드 채택 알고리즘 분류

기반문제	기능		계
	공개키 암호/키 설정	전자서명	
격자	2	5	7
코드	4	1	5
다변수	-	1	1
해시	-	1	1
아이소제니	1	1	2
기타	1	1	2
계	**8**	**10**	**18**

- 암호알고리즘의 우수성, 독창성
- 기반 문제를 통한 안전성 근거의 타당성
- 개발 목표의 구체성, 실현 가능성 및 개발 계획의 적절성

채택된 18종을 기반문제와 기능별로 분류하면 [표 5]와 같다. [표 5]에서 알 수 있듯이 기반문제가 격자, 코드, 다변수, 해시, 아이소제니 등으로 다양하며 공개키 암호, 키 설정, 전자서명이 골고루 제안되었다. 채택된 알고리즘은 KpqC 공모전 1라운드에 참여할 수 있는 자격이 부여되었다.

3.2. 공모전 1라운드

3.2.1. 1라운드 제출 알고리즘

KpqC 연구단은 국내 상황을 고려하며 공모전을 운영하고자 0라운드 기간에 공모전 참여자를 대상으로 1라운드 관련 의견을 수렴하였고, 이를 반영하여 알고리즘 상세서의 세부 양식 등을 수정하였다.

1라운드 제출물은 다음과 같다.

- 알고리즘 상세서
- 참조구현 코드
- KAT 값

1라운드에는 [표 6]과 같이 총 16종의 알고리즘이 제안되었다. 이를 기능과 기반문제 별로 분류하면 [표 7]과 같다. 16종 중 격자 기반 알고리즘이 8종으로 가장 많았고, 코드 기반 알고리즘이 4종, 이 외에 다변수 기반, 아이소제니 기반, 영지식 증명, 그래프 기반의 알고리즘이 각 1종씩 제안되었다.

1) 연구단 이메일(kpqcrypto@gmail.com)로 접수

〔표 6〕 1라운드 채택 알고리즘명

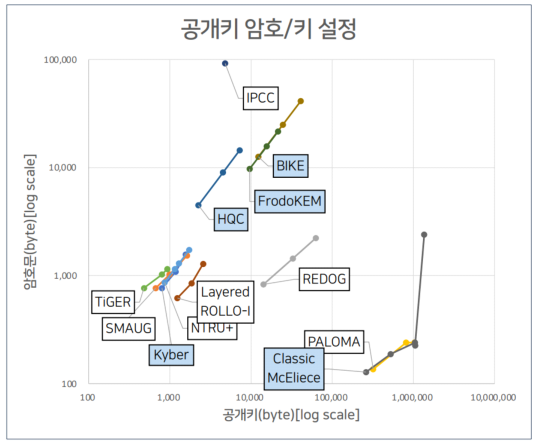
알고리즘 명[2]	기능	기반문제
IPCC*	공개키 암호	기타 (그래프)
Layered ROLLO-I*†	키 설정	코드
NTRU+	공개키 암호	격자
PALOMA	키 설정	코드
REDOG	공개키 암호	코드
SMAUG*†	키 설정	격자
TiGER*	키 설정	격자
AIMer	전자서명	기타 (영지식증명)
Enhanced pqsigRM	전자서명	코드
FIBS	전자서명	아이소제니
GCKSign*	전자서명	격자
HAETAE†	전자서명	격자
MQ-Sign*	전자서명	다변수
NCC-Sign	전자서명	격자
Peregrine*	전자서명	격자
SOLMAE	전자서명	격자

〔표 7〕 1라운드 채택 알고리즘 분류

	공개키 암호/키 설정	전자서명	계
격자	3	5	8
코드	3	1	4
다변수	-	1	1
아이소제니	-	1	1
기타	1	1	2
계	**7**	**9**	**16**

양자내성암호 국가공모전 1라운드와 NIST PQC 표준화 공모전에 제안된 주요 공개키 암호/키 설정 알고리즘의 암호문과 공개키 크기는 [그림 2]에서 쉽게 비교할 수 있다. 격자 기반 알고리즘인 TiGER, SMAUG, NTRU+가 비교적 작은 공개키와 암호문 크기를 가졌고, 코드 기반 알고리즘인 Layered ROLLO-I, REDOG, PALOMA는 대부분 공개키 크기가 큰 편이나 암호문의 크기는 작은 편에 속한다. PALOMA는

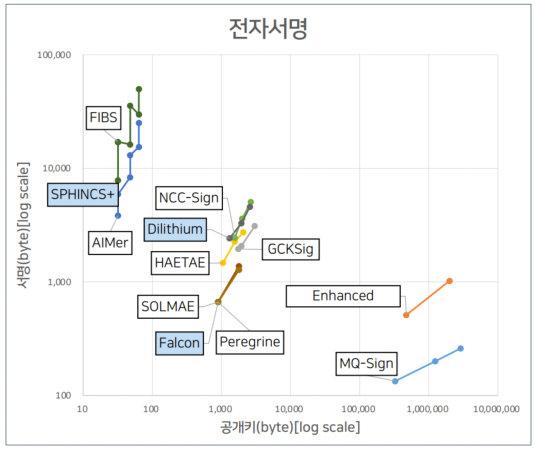
2) * : '23년 5월 기준 KpqC Bulletin Board에 코멘트 게시글이 있는 알고리즘
† : '23년 5월 기준 업데이트 한 알고리즘



〔그림 2〕 1라운드 공개키 암호/키 설정 알고리즘의 암호문과 공개키 크기 비교(Bytes)

공개키 크기가 비교적 크지만 암호문의 크기는 제출된 알고리즘 중 가장 작은 특징이 있고, 그래프 기반 알고리즘 IPCC는 암호문의 크기가 매우 큰 특징을 가지고 있다.

전자서명 알고리즘의 공개키와 서명의 크기는 [그림 3]에서 쉽게 비교할 수 있다. 격자 기반 알고리즘인 NCC-Sign, HAETAE, SOLMAE, Peregrine, GCKSign은 공개키의 크기가 유사하며, 코드 기반 알고리즘인 Enhanced pqsigRM과 다변수 기반 알고리즘인 MQ-Sign은 공개키 크기가 비교적 큰 편에 속한다. MQ-Sign은 제안된 알고리즘 중 가장 작은 서명을 제공하고 있으며, 아이소제니 기반 FIBS와 영지식증명을 사용하는 AIMer는 공개키의 크기가 작고 서명의



〔그림 3〕 1라운드 전자서명 알고리즘의 서명과 공개키 크기 비교(Bytes)

크기가 크다는 특징을 가지고 있다.

3.2.2. 1라운드 알고리즘 분석 및 평가 방안

16종의 알고리즘은 2022년 12월 5일에 KpqC 연구단 홈페이지[3]에 게시되어 현재 공개 검증 중이다. 로그인 과정이나 가입 없이 누구나 알고리즘 상세서, 참조구현 코드, KAT 값을 홈페이지에서 다운로드 할 수 있으며, 알고리즘 관련 연구 결과를 공유하고자 한다면 KpqC 연구단에서 운영 중인 'KpqC Bulletin Board[4]'에 가입한 후 게시할 수 있다. 단, 게시의 목적이 아니라 게시글을 열람만 하고자 한다면 별도의 가입 절차 없이 누구나 확인 가능하다. 2023년 5월을 기준으로 총 8개의 알고리즘에 관한 18개의 게시글이 올라와 있으며, 이 중 7개의 게시글은 7개의 알고리즘에 대한 안전성 분석 결과에 관한 것이다.

이러한 공개검증 방법은 NIST PQC 표준화 공모전에서 사용된 검증 방법과 유사하다. 공개검증은 불특정 다수에게 정보를 공유함으로 정보의 전파력이 크고 대중의 전문지식 분야 및 수준의 다양함을 활용할 수 있다는 측면에서 의미 있지만, 특정 알고리즘에 관심이 편중되거나 혹은 일부 알고리즘의 분석이 충분히 이루어지지 않을 수 있다는 우려가 있다. 이에 KpqC 연구단은 공개검증과 더불어 연구단 세부과제 발주 및 해외 전문 연구기관에 알고리즘 분석을 의뢰하여 모든 알고리즘에 대해 일정 수준 이상의 분석이 이루어지도록 노력하고 있다.

해외 전문 연구기관으로는 네덜란드의 Eindhoven 공과대학의 Tanja Lange 교수 연구팀이 현재 16개의 알고리즘에 대하여 안전성 분석을 진행하고 있으며, 연구팀의 참여 교수진은 [표 8]과 같다.

이 외에도 국내 KpqC 알고리즘 분석을 활성화하기 위하여 2023년에는 국가암호공모전에 KpqC 1라운드 알고리즘과 관련한 C분야를 새로 개설하였다. A분야와 B분야는 예년과 동일하게 대학생, 대학원생, 박사후연구원을 대상으로 진행되는 반면, C분야는 산업체 재직자도 대상자에 추가하여 진행된다[5].

KpqC 연구단은 1라운드 알고리즘 선정 시 다음과 같이 여러 채널의 결과를 반영할 예정이다.

〔표 8〕 Eindhoven 공과대학 Lange 교수 연구팀

	이름	전문 분야
연구 책임자	Tanja Lange	양자내성암호, 응용 암호, 수론
참여 교수	Kathrin Hövelmanns	암호 안전성 증명
	Andreas Hülsing	암호 안전성 증명, 응용 암호
	Alberto Ravagnani	오류 정정 부호 이론
	Sven Schäge	암호 안전성 증명, 응용 암호
	Benne de Weger	양자내성암호, 응용 암호, 수론

- 국외 전문 연구기관의 분석 결과
  - Eindhoven 공과대학의 Tanja Lange 교수 연구팀에 분석 의뢰
- 1라운드 평가위원단 심사 결과
  - 알고리즘 개발 참여자를 제외한 다양한 분야 전문가로 구성하여 심사
- 연구단 세부 과제를 통한 평가·분석 결과
  - 알고리즘 평가·분석 관련 세부과제 추진
- 국내외 공개 학술 및 발표 결과
  - Archive, 학회, 저널, KpqC Bulletin Board 등에 공개된 결과 반영
- 국가암호공모전 결과
  - C분야(KpqC 1라운드 알고리즘 관련 분야)를 통해 선정된 우수 연구 결과 반영

1라운드 알고리즘의 평가 기준은 다음과 같다.

- 안전성
  - 안전성 정의에 대한 증명
  - 정량적 안전성에 대한 근거
- 독창성
- 다양한 환경에서의 활용성
- 효율성
  - 구성 요소의 크기
  - 복호화 실패 확률
  - 참조 구현 동작 효율성

1라운드 알고리즘 선정 결과는 2023년 12월에 발표될 예정이다.

3) www.kpqc.or.kr
4) www.groups.google.com/g/kpqc-bulletin
5) 국가암호공모전의 대상자는 주저자에 대한 기준이다.

3.3. 공모전 일정

2021년에 시작한 양자내성암호 국가공모전은 2023년 12월에 1라운드 선정 알고리즘을 발표한 후 2024년 2월부터 9월까지 2라운드를 진행한다[표 9]. 현재는 2라운드에서 최종 알고리즘을 선정하는 것으로 계획되어 있으나, 선정된 알고리즘을 국가 및 공공기관에 적용하는 데 필요한 사항을 준비하기 위한 3라운드 진행 여부를 검토하고 있다.

Ⅳ. 결 론

공개키 암호체계의 해독 여부로 직결되는 양자컴퓨터의 실용화 시기는 기술적으로 다양하게 검토되어야 할 문제이다. 정확한 시기를 예측하기는 어렵겠지만 현 공개키 암호체계에 미치게 될 파급효과를 고려하였을 때, 양자컴퓨터가 언젠가는 개발된다는 전제하에 PQC로의 전환을 충실히 준비해야 할 것으로 판단된다.

한편, PQC 알고리즘이 표준화된 이후 구현과 각종 프로토콜, 네트워크 및 시스템에 장착되기까지 많은 시간이 소요될 것으로 예상된다. 아직은 낮은 성숙도로 인해 알려지지 않은 다른 요인에 의해 안전성 문제가 발생 할 수도 있다. 따라서, PQC 알고리즘은 다양한 형태로 개발되는 것이 바람직하며, 개발 완료 이후의 PQC 전환에 필요한 기술 개발 및 관련 정책의 마련 또한 사전에 준비해야 할 것으로 보인다.

〔표 9〕 양자내성암호 국가공모전 일정

시기	내용
'21.5.21.	공모전 계획 발표(서울, KpqC 1차 워크숍)
'21.11.26.	공모전 개최 공지(평창, KpqC 3차 워크숍)
'21.11.25.	공모전 홈페이지 오픈
'22.2.18.	0라운드 개발계획서 접수 마감
'22.3.18.	평가위원회 심사 및 0라운드 결과 통보 (18종 알고리즘)
'22.10.31.	1라운드 제안서 제출 마감 (16종 알고리즘)
- KpqC 공모전 1라운드 -	
'22.12.5.	국내외 공개검증 시작
'22.12.26.	KpqC Bulletin Board 운영 (알고리즘 토론의 장)
'23.4.19.	국가암호공모전 논문모집 공고 (C분야: KpqC 알고리즘 분야)
'23.12.	공모전 1라운드 결과 발표(예정)
'24.2.	'2라운드 제안서' 접수 마감
- KpqC 공모전 2라운드 -	
'24.9.	KpqC 공모전 최종 결과 발표(예정)

인위적으로 PQC 알고리즘 개발을 지연시킬 필요는 없지만, 반대로 너무 서둘러 개발을 시도하는 경우 안전성이나 효율성의 문제를 야기할 가능성이 있을 것으로 판단된다. KpqC 연구단은 지금까지 그래왔듯이 앞으로도 다양한 채널을 통하여 의견을 수렴하고 국내외 동향을 파악하며 국내 상황을 고려하는 방향으로 공모전을 진행할 예정이다. 무엇보다도 공모전 진행 과정을 통하여 국내 PQC 분야가 활성화되고 관련 기술의 경쟁력이 강화되기를 희망한다.

참 고 문 헌

[1] P. Shor, “Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer”, *SIAM J. Comput.,* 26(5), pp. 1484-1509, 1997.

[2] L. K. Grover, “A fast quantum mechanical algorithm for database search”, *Proceedings, 28th Annual ACM Symposium of the Theory of Computing*, pp. 212, 1996.

[3] M. Mosca, “Setting the Scene for the ETSI Quantum-safe Cryptography Workshop“, *e-proceedings of the 1st Quantum-Safe-Crypto Workshop*, pp. 26-27, 2013.

[4] The White House, “National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems”, 2022.

[5] NSA, “NSA Releases Future Quantum-Resistant (QR) Algorithm Requirements for National Security Systems”, 2022. Available at https://www.nsa.gov/Press-Room/News-Highlights/Article/Article/3148990/nsa-releases-future-quantum-resistant-qr-algorithm-requirements-for-national-se/

[6] BSI, “Cryptographic Mechanisms: Recommendations and Key Lengths”, 2023. Available at https://www.bsi.bund.de/SharedDocs/Downloads/EN/BS

I/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.pdf?__blob=publicationFile&v=6

[7] NLNCSA, “Prepare for the threat of quantum computers”, 2022. Available at https://english.aivd.nl/publications/publications/2022/01/18/prepare-for-the threat-of-quantumcomputers

[8] ANSSI, “ANSSI views on the Post-Quantum Cryptography transition”, 2022. Available at https://www.ssi.gouv.fr/uploads/2022/01/anssi-technical_position_papers-post_quantum_cryptography_transition.pdf

〈저 자 소 개〉

이 나 리 (Nari Lee)

2009년 2월 : 서강대학교 수학과 졸업
2011년 2월 : 서강대학교 수학과 석사
2017년 8월 : 서강대학교 수학과 박사
2017년 12월~현재 : ETRI 부설연구소 선임연구원
<관심분야> 양자내성암호, 부호이론, 조합론 등

정 경 철 (Kyung Chul Jeong)

종신회원

2005년 2월 : 서울대학교 수리과학부 졸업
2011년 2월 : 서울대학교 수리과학부 박사 (석박통합)
2010년 12월~현재 : ETRI 부설연구소 실장
<관심분야> 양자내성암호, 암호분석 등

지 성 택 (Seongtaek Chee)

종신회원

1985년 2월 : 서강대학교 수학과 졸업
1987년 2월 : 서강대학교 수학과 석사
1999년 2월 : 고려대학교 수학과 박사
1989년 10월~현재 : ETRI 부설연구소 책임연구원
<관심분야> 암호, 정보보호 등

한 대 완 (Daewan Han)

1995년 2월 : 서울대학교 수학과 졸업
1997년 2월 : 서울대학교 수학과 석사
2007년 2월 : 서울대학교 수학과 박사
2001년 3월~현재 : ETRI 부설연구소 센터장
<관심분야> 암호, 정보보호 등