양자내성암호 기술 개발 및 표준화 동향

심경아
국가수리과학연구소

요 약

양자컴퓨터의 등장은 기존 컴퓨팅 기술의 한계를 극복하고 전 산업에 큰 파급 효과가 예상되지만, 현재 사용하고 공개키 암호 체계 무력화를 초래하는 양면성을 가지고 있다. 양자컴퓨팅 기술의 발전으로 인한 양자컴퓨터의 출현은 현재 사용하고 있는 공개키 암호알고리즘의 붕괴를 예고하고 있다. 이는, 인터넷 쇼핑, 뱅킹 등의 전자상거래와 암호통신이 더 이상 안전하지 않음을 의미하는 것으로, 양자컴퓨터 이후 시대의 안전한 통신과 정보보호를 위해 모든 보안 분야에서 양자컴퓨터 공격에 대응 가능한 양자내성암호로 반드시 교체되어야 한다. 본고에서는 양자내성암호 기술 개발 및 표준화 동향에 대해 살펴보고자 한다.

Ⅰ. 서 론

양자컴퓨팅 기술의 발전으로 인한 양자컴퓨터의 출현은 현재 사용하고 있는 공개키 암호알고리즘의 붕괴를 예고하고 있다. 공개키 암호알고리즘의 안전성은 기본 논리로 사용되는 수학적 난제에 의존하고 있으며, 사용된 수학적 난제가 해결되면 암호알고리즘도 깨지게 되는 구조를 가지고 있다. 현재 국제표준 공개키 암호인 RSA와 ECDSA 등의 안전성은 소인수분해문제 및 이산대수문제에 기반을 두고 있는데, 큰 규모의 양자컴퓨터 개발이 완료되면 Shor 알고리즘[1]에 의해 이 난제들은 쉽게 풀리고, 국제표준 공개키 암호도 실시간 해독이 가능해져 사용할 수 없게 된다는 것이 알려져 있다. 이는, 인터넷 쇼핑, 뱅킹 등의 전자상거래와 암호통신이 더 이상 안전하지 않음을 의미하는 것으로, 양자컴퓨터 시대 이후 사이버 세계의 통신 대란을 예고하고 있어 이에 대응 가능한 양자컴퓨터에 안전한 암호알고리즘으로 반드시 교체해야한다.

본고에서는 양자컴퓨터 공격을 실현시키는 양자알고리즘과 양자내성암호 기술 개발 동향과 표준화 현황에 대해 알아보고자 한다. II장에서 양자 알고리즘과 양자내성암호 개발 동향을 III장에서는 양자내성 암호 표준화 동향을 살펴본다. IV장에서는 본고의 결론을 제시한다.

Ⅱ. 양자 알고리즘과 양자내성암호 개발 동향

1. 양자컴퓨터 출현과 양자 알고리즘

가. 양자컴퓨터의 출현

양자컴퓨팅 기술의 발전은 양자컴퓨터 시대의 개막을 준비하고 있다. 2019년 구글은 네이처에 양자우월 (Quantum supremacy)을 달성했다고 발표하였다[2]. 이 논문에서는 현재 가장 빠른 슈퍼컴퓨터로 만년이 걸리는 연산을 54 큐빗 시커모어 프로세서로 단 200초 만에 수행해 양자 기술의 우위를 증명하였다. IBM은 'IBM 퀀텀 서밋 2022'에서 433 큐빗 IBM 오스프리 양자 프로세서와 차세대 양자컴퓨터'IBM 퀀텀 시스템 투'를 발표했다. IBM은 2023년 1121 큐빗 콘도르의 개발을 예고하였고, 세계 최대 정보기술(IT)·가전 전시회"CES 2021"에서는 2030년까지 100만 큐빗 달성을 선언한 바 있다.

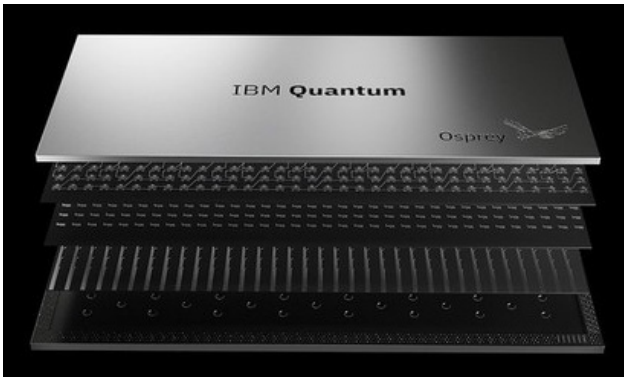

그림 1. IBM 이 양자 프로세서 오스프리

나. 양자 알고리즘

1997년 Shor가 큰 규모의 양자컴퓨터가 개발이 되면 소인수분해문제와 이산대수문제를 다항식 시간 안에 해답을 찾을 수 있는 양자알고리즘을 제안하였고, Grover는 검색 문제의 복잡도를 향상시키는 양자알고리즘을 제안하였다. 양자알고리즘 소개와 대응 방안에 대해 논하기 전에 암호알고리즘의 종류를 살펴보도록 하겠다. 암호알고리즘은 아래와 같이 크게 두 종류로 나눌 수 있다.

- 대칭키 암호(symmetric-key cryptography): 송신자와 수신자가 동일한 비밀키를 가지고 암호화와 복호화를 수행하는 암호화 알고리즘으로, 알고리즘 수행 전에 통신 당사자들 간의 사전 키분배가 요구되는 단점이 있다. 현재 국제 표준 대칭키 암호 AES가 전 세계적으로 사용되고 있다.
- 공개키 암호(public-key cryptography, asymmetric key cryptography): 통신 당사자들 간의 사전 키분배 문제를 해결하기 위해 사용자의 공개키/비밀키 쌍을 만들어, 암호화 알고리즘의 경우 송신자는 공개키를 사용하여 암호화를 수행하고 수신자는 공개키에 대응되는 비밀키를 사용하여 복호화를 수행한다. 종류로는 암호화 알고리즘, 전자서명 알고리즘, 키공유 알고리즘이 있다. 현재 국제 표준 공개키 암호는 RSA, ECDSA, (EC)DH 키교환 알고리즘이 전 세계적으로 사용되고 있다.

국제 표준 공개키 암호는 현재의 계산 능력으로는 해결하기 어려운 수학적 난제인 소인수분해 문제와 이산대수 문제에 기반을 두고 있다. 공개키 암호알고리즘의 안전성은 기본 논리로 사용되는 수학적 난제에 의존하고 있으며, 사용된 수학적 난제가 해결되면 암호알고리즘도 깨지게 되는 구조를 가지고 있다. 두 난제는 아래와 같이 정의된다.

- 소인수분해 문제: 합성수 $N = p \cdot q$ 가 주어져 있을 때, 소인수를 p, q를 찾는 문제
- 이산대수 문제: 군, 생성자와 군의 원소 $(G,\ g, g^x)$ 가 주어져 있을 때, g^x의 이산 로그 x를 찾는 문제

대칭키 암호와 공개키 암호에 안전성에 영향을 미치는 양자알고리즘은 Shor 알고리즘과 Grover 알고리즘이 있다.

- Shor 알고리즘[1]: 소인수분해문제와 이산대수문제를 다항식 시간 안에 해답을 찾을 수 있는 양자알고리즘으로 소인수분해문제 기반인 RSA와 이산대수문제 기반인 DSA, ECDSA 전자서명 알고리즘과 Diffie-Hellman 키분배 알고리즘에 적용할 수 있다.
- Grover 알고리즘[3]: 기본적인 검색 알고리즘의 복잡도를 N에서 $\sqrt{N}$으로 향상시켜주는 양자알고리즘으로 대칭키 암호 알고리즘과 해쉬 함수 등 모든 전수조사에 적용 가능하다.

다. 양자 알고리즘에 대한 대응

위의 두 종류의 양자알고리즘에 대한 대칭키 암호와 공개키 암호의 대응법은 아래와 같다.

- 대칭키 암호 알고리즘: 양자컴퓨터를 이용한 공격, 즉, Grover 알고리즘에 대응하기 위해서는 대칭키 암호 알고리즘, 해쉬 함수 등은 키 크기를 2배 이상 늘려서 이전과 동일한 수준으로 안전성을 확보할 수 있다.
- 공개키 암호알고리즘: 현재 사용 중인 모든 국제표준 공개키 암호는 소인수분해문제와 이산대수문제에 기반을 두고 있어 양자컴퓨터의 개발이 완료되면 Shor 알고리즘에 의해 다항식 시간 안에 깨지므로 키 길이를 늘이는 것으로 대응할 수 없어 모두 양자컴퓨터에 안전한 공개키 암호로 교체되어야 한다.

2. 양자내성암호 개발 동향

먼저, 양자내성암호를 정의하고, 양자내성암호의 연구 동향과 최신 공격 동향을 살펴본다.

가. 양자내성암호 정의

양자내성암호 (PQC: Post-Quantum Cryptography)의 정의는 현재의 컴퓨터를 이용한 공격과 양자컴퓨터를 이용한 공격에 모두 안전한 수학적 난제의 어려움에 기반한 공개키 암호알고리즘을 의미한다.

나. 양자내성암호의 종류

양자내성암호는 양자컴퓨터에 안전하다고 알려진 수학적 난제에 기반을 둔 공개키 암호인데, 양자컴퓨터에 안전하다고 알려진 수학적 난제는 양자컴퓨터가 효율적으로 풀 수 있는 난제의 집합인"BQP (Bounded error, Quantum, Polynomial time)"에 속하지 않는 NP-hard, NP-complete 문제에 기반을 두고 있다. 양자내성암호는 기반이 되는 수학적 난제에 따라 다변수 이차식 기반, 격자 기반, 코드 기반, 해쉬 함수 기반, 아이소제니 기반으로 나누어져 활발하게 연구가 진행되고 있다. 각 양자내성암호의 기반 문제는 다음과 같다.

- 해쉬 함수 기반 (hash function-based)[4]: 해쉬 함수 H가 주어졌을 때, $H(x) = H(x')$ 을 만족하는 충돌쌍 $(x,\ x')$을 찾는 문제(collision resistance)에 기반을 둔 암호로 전자서명 알고리즘만 연구되고 있다.
- 다변수 이차식 기반 (multivariate quadratic equation-based)[5]: 유한체에서 정의된 다변수 이차식 시스템의 해를 구하는 문제에 기반을 둔 암호로 이차 다항식의 특성 상 일대일 함수가 아니어서 암호화 알고리즘 개발이 어려운 구조이며 주로 전자서명 알고리즘이 연구되고 있다.

〈표 1〉 양자내성암호 장·단점 비교 분석

구분	장점	단점
해쉬 함수 기반	해쉬 함수 관련 어려움만 요구 다른 난제의 어려움을 요구하지 않아 강한 안전성 제공	전자서명만 존재 stateful 전자서명: 일회용 전자서명 기반 stsate 유지 필요 stateless 전자서명: stsate 유지가 필요 없지만 서명의 길이가 길고 속도가 느림
다변수 이차식 기반	전자서명의 길이가 가장 짧고, 속도가 빠르고, 구현이 용이	키길이가 길고, 이차식의 구조로 암호화 알고리즘 설계가 어려움
격자 기반	키길이, 전자서명 길이, 속도가 상대적으로 짧고 빠름. 암호화/전자서명/동형암호 등 다양한 종류의 암호 설계 가능	대부분의 효율적인 알고리즘이 구조화된 격자를 이용 잠재적인 위협 존재
코드 기반	코드 기반 암호화 알고리즘의 경우 안전성 검증이 오래되었다는 장점	전자서명 알고리즘의 설계가 어렵고, 키길이가 길다
Supersingular-isogeny 기반	타원곡선 암호 연구의 연장선상에 있다는 장점	신생 문제로 검증 기간이 짧다는 단점

- 격자 기반 (lattice-based)[6]: 가장 짧은 길이의 벡터를 찾는 문제(shortest vector problem)에 기반한 암호로 암호화/전자서명 알고리즘 개발에 모두 이용되고 있으며, 다양한 대수적인 구조를 이용한 동형암호(homomorphic encryption) 등 특별한 성질을 만족하는 여러 종류의 암호알고리즘 개발에 활발하게 이용되고 있다.
- 코드 기반 (code-based)[7]: 일반적인 선형 코드 (linear Code)를 디코딩 하는 문제 (syndrome decoding problem)에 기반을 둔 암호로 암호화/전자서명 알고리즘 개발에 모두 이용되고 있다.
- Supersingular-isogeny 기반 (supersingular Isogeny-based)[8]: supersingular 타원곡선에서 isogeny를 찾는 문제에 기반을 둔 암호로 키분배 알고리즘 의 개발에 이용되고 있다.

〈표 1〉은 다섯 가지의 문제 기반 양자내성암호의 장·단점을 비교 분석한 것이다.

다. 양자내성암호 최신 공격 동향

미국 NIST가 양자내성암호 표준화 공모 프로젝트를 진행하는 동안 양자내성 후보 알고리즘에 대한 다양한 공격이 발표되었다. 그 중 대표적인 것이 NIST 3 라운드 최종 후보였던 Rainbow에 대한 공격와 NIST 4 라운드 최종 후보로 선정된 SIKE에 대한 공격이다. 최근 발표된 진화된 공격들을 살펴보자.

- Rainbow에 대한 공격: Rainbow는 유한체에서 정의된 다변수 이차식 시스템의 해를 구하는 문제의 어려움에 기반을 둔 전자서명 알고리즘이다[9]. 작은 유한체를 사용하여 구현이 용이하고, 키길이가 큰 단점이 있으며, 전자서명의 길이가 알려진 양자내성 전자서명 중에서 가장 짧고, 서명 생성/검증 성능이 우수하다는 장점이 있다. 최근, Rainbow의 다중 레이어 구조를 이용한 Rainbow-Band-Separation 공격, MinRank 공격 등이 발표되었고[10], Ward의 simple 공격으로 NIST 2 라운드 제출 안전도 1의 파라미터가 랩 탑에서 53 시간 만에 해결하는 결과가 발표되었다[11]. 이에, Rainbow 개발 팀은 안전도 3과 5의 파라미터를 각각 안전도 1과 3의 파라미터로 변경하겠다고 발표하였다. 파라미터의 변경으로 안전성은 확보하였지만 다중 레이어 구조를 이용하지 않는 다변수 이차식 기반 전자서명과 비교했을 때 효율성이 떨어져 장점이 사라졌으며, 결국 NIST 양자내성암호 공모 프로젝트 4 라운드에 선정되지 못했다.
- SIKE에 대한 공격: Supersingular-isogeny 기반 키설정 알고리즘인 SIKE는 NIST 4 라운드 선정 직후 등장한 공격에 완전히 깨진 상황이다. Kani의 "glue-and-split"정리를 이용한 공격으로 안전도 1의 파라미터 SIKEp434를 단일 코어에서 1시간 내에 비밀키 복구에 성공하였고, 안전도 2의 파라미터 SIKEp503, 안전도 3의 파라미터 SIKEp610, 안전도 5의 파라미터 SIKEp751도 각각 2시간 19분, 8시간 15분, 20시간 37분의 시간으로 비밀키 복구에 성공하였다[12]. 공격 내용의 유효성은 검증이 되었고, SIKE의 변형된 버전은 위의 공격을 막을 수 있다고 기술되어 있었지만 변형된 버전마저 공격된 논문이 발표되었다[13]. SIKE의 취약점이 드러남에 따라 NIST 4 라운드의 후보들에 대한 다양성과 신뢰성이 일부 훼손되었다고 볼 수 있다.

Ⅲ. 국내·외 양자내성암호 표준화 현황

1. 미국 NIST 표준화 현황

미국 NIST (National Institute of Standards and Technology)는 2016년 차세대 암호알고리즘 표준화를 목적으로 양자컴퓨터에 안전한 암호화 알고리즘, 전자서명 알고리즘, 키분배 알고리즘의 공모를 시작하였다. 2016년 11월 30일까지 25개 나라에서 총 82개의 알고리즘이 제출되어, 2017년 1라운드 64개의 알고리즘을 선정하였고, 2019년 2라운드 26개 알고리즘을 선정하였고, 2020년 3라운드 7개 최종 후보 알고리즘과 8개의 대안 알고리즘을 선정하였고, 2022년 7월 1종의 암호화/키설정 알고리즘과 3종의 전자서명 알고리즘을 선정하여 표

준화를 시작하겠다고 발표하였다. 추가적으로 4 라운드 후보알고리즘으로 4개의 암호화/키설정 알고리즘을 발표하였고, 검증을 진해하고 최종 알고리즘으로 선정한 후 표준화를 진행할 예정이다. NIST 4 라운드에 선정된 4종의 알고리즘과 후보 알고리즘에 대한 상세 설명은 아래와 같다.

- CRYSTALS-Kyber: 격자 기반 암호화/키설정 알고리즘으로 Module-LWE, Module-SIS 문제의 어려움에 기반을 두고 있다. 구조화된 격자를 이용하고 있고, 키길이, 암호문 길이, 암/복호화 속도가 상대적으로 짧고 효율적이다.
- CRYSTALS-Dilithium: 격자 기반 전자서명 알고리즘으로 Module-LWE, Module-SIS 문제의 어려움에 기반을 두고 있다. CRYSTALS-Kyber에서처럼 구조화된 격자를 이용하고 있고, 키길이, 전자 서명의 길이, 서명 생성/검증 속도가 상대적으로 짧고 효율적이다. 설계 구조는 Fiat-Shamir with aborts 방법을 따르고 있다.
- Falcon: 격자 기반 전자서명 알고리즘으로 NTRU 문제의 어려움에 기반을 두고 있다. CRYSTALS-Dilithium에서처럼 구조화된 격자를 이용하고 있고, CRYSTALS-Dilithium 보다 키길이와 전자 서명의 길이는 짧고, 서명 생성 속도는 느리다. 설계 구조는 Hash-and Sign 방법을 따르고 있다. floating point를 사용하는 등 구현이 매우 복잡하고 비효율적이다.
- SPHINCS+: 해쉬 함수의 두번째 역상을 찾는 문제의 어려움(Second preimage resistance)에 기반을 두고 있다. 다른 난제 기반 전자서명 알고리즘들도 부가적으로 해쉬 함수의 충돌 저항성(collision resistance)을 요구하고 있는 상황에서, 해쉬 함수 기반의 전자서명 알고리즘은 다른 문제의 어려움을 요구함이 없이 해쉬 함수 자체 문제의 어려움만을 요구한다는 측면에서 강한 안전성을 제공한다고 장점이 있다. 그러나, 서명의 길이가 수십 KB를 넘어가고, 연산에서 450,000 번의 해쉬 연산과 90,000 번의 다른 해쉬 연산을 반복 수행으로 인해 속도가 느리다는 단점이 있다.
- BIKE, Classic McEliece, HQC(코드 기반): 암호화/키설정 알고리즘으로 일반적인 선형 코드 (linear Code)를 디코딩하는 문제 (syndrome decoding problem) 등의 어려움에 기반을 두고 있다. 특히, Classic McEliece의 경우 오랫 동안 안전성 검증이 이루어졌다는 장점이 있지만, 키길이가 커서 범용으로 사용하기 어렵다고 판단되어지고 있다. NIST는 4라운드 분석 및 검증을 통해 최종적으로 선정하겠다고 발표하고 있다.
- SIKE: 키설정 알고리즘으로 Supersingular- isogeny 문제의 어려움에 기반을 두고 있다. 다른 난제들에 비해 안전성 검증의 역사가 짧고, 속도가 느리다는 단점이 있다.

〈표 2〉는 NIST 4라운드 최종 후보 및 후보 알고리즘을 정리한 것이다.

표 2. NIST 4라운드 최종 후보 및 후보 알고리즘[14]

구분	암호화/키설정 알고리즘	전자서명 알고리즘
최종 알고리즘	CRYSTALS-Kyber (module 격자 기반)	CRYSTALS-Dilithium (module 격자 기반)
		Falcon (NTRU 격자 기반)
		SPHINCS+ (해쉬 함수 기반)
후보 알고리즘	BIKE, Classic McEliece, HQC(코드 기반)	다양성 위한 전자서명 알고리즘 재공모 계획 발표
	SIKE(supersingular isogeny 기반)	

NIST의 후보 양자내성암호들은 대부분 구조가 있는 격자(structured lattices: module lattice, NTRU lattice)를 이용하고 있어, 이 특별한 구조를 이용한 잠재적인 공격에 대한 우려와 모든 종류의 양자내성암호가 한 가지 난제에 의존할 경우 생길 수 있는 위협에 대한 우려를 하고 있다. 전자서명 알고리즘의 경우 대안 알고리즘 중 해쉬 함수 기반 SPHINCS+를 4라운드에 최종 선발에 추가하였고, 전자서명 알고리즘의 다양성을 위해 구조화된 격자를 이용하지 않으면서, 서명의 길이가 짧고 서명 검증이 빠른 새로운 전자서명 알고리즘을 2023년 6월까지 재공모 하겠다는 계획을 발표하였다.

가. IETF 표준화 현황

해쉬 함수 기반 stateful 전자서명 알고리즘 XMSS[15], XMSS^MT[16], LMS[17] 표준으로 제정되었는데, 이 전자서명 알고리즘들은 일회용 전자서명 (one-time signature)을 사용하고 있어 한 번 사용한 비밀키를 재사용하는 경우 안전성이 보장되지 않아 비밀키 업데이트를 위한 안전한 state의 관리를 요구하고 있고, 서명할 수 있는 메시지의 개수에 제한이 있다는 단점을 가지고 있다.

2. 국내 TTA 표준화 현황

국내에는 양자내성암호는 전자서명 알고리즘과 암호화 알고리즘이 정보통신단체표준으로 제정되어 있다.

- S전자서명 알고리즘: 정보통신단체표준(TTAS), TTAK.KO-12.0348-Part2: 다변수 이차식 기반 양자내성암호-제2부: HiMQ, 부가형 전자서명 알고리즘[18]

- S암호화 알고리즘: 정보통신단체표준(TTAS), TTAK.KO-12.0349-Part2격자 기반 양자내성암호 - 제2부: 링-리자드(Ring-Lizard) 알고리즘[19]

3. 양자내성암호로 전환

위에서 언급했듯이 양자컴퓨터 시대 이후의 안전한 암호 통신과 정보보호를 위해서는 대칭키 암호와 해쉬 함수 등은 키길이를 2배 이상 늘려주어야 하고, 공개키 암호를 사용하고 있는 분야는 현 국제표준 공개키 암호를 양자컴퓨터에 안전한 공개키 암호알고리즘으로 반드시 교체해야한다. 전환 단계는 hybrid 전환과 완전한 전환으로 나누어진다.

- Hybrid 전환: 기존 국제표준 공개키 암호와 양자내성암호를 동시에 사용하면서 백워드 호환성 (backward compatability)을 달성하면서, 장기간 안전성 (long-term security)을 요구하는 분야에는"지금 저장해 놓고, 나중에 깨는 (Store now, break later)"공격을 막기 위해 양자내성암호 선제적으로 사용하는 기간을 의미한다.
- 완전한 전환: 모든 분야에서 양자내성암호로 전환하는 시기로, NIST는 2031년으로 계획하고 있다.

〈그림 2〉는 2013년 Waterloo 대학의 Michele Mosca가 제시한 양자컴퓨터 공격에 대비하기 위한 시간을 계산하는 식을 나타낸다. x는 데이터가 암호알고리즘 사용으로 보호되어야 하는 기간, y는 양자내성암호로의 전환에 소요되는 기간, z는 양자컴퓨터 개발 완료까지의 기간을 의미한다. 데이터 보호 기간과 전환 소요 기간을 합한 시간이 양자컴퓨터 개발 속도보다 크다면 ($y + x > z$), 안전하지 못하다는 것을 의미한다. 그러므로, 기존 암호알고리즘의 사용으로 암호화된 데이터의 유효한 기간과 데이터 저장, 보호 기간, 양자컴퓨터 개발까지의 기간을 고려하여 우선순위를 정하고 그 순서에 따라 순차적인 전환이 필요하다.

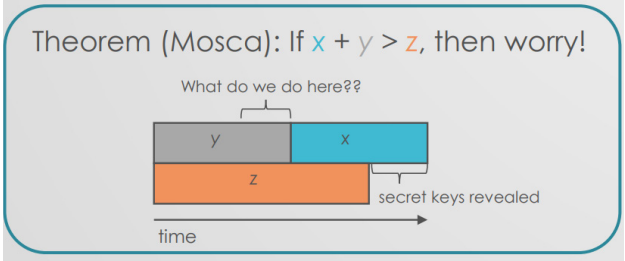

그림 2. Mosca 공식(THE SHIP HAS SAILED, NIST[20])

IV. 결 론

본고에서는 양자컴퓨터에 안전한 수학적 난제 기반 공개키 암호인 양자내성암호의 기술 개발 동향과 표준화 현황에 대해 살펴보았다. 양자컴퓨터의 개발이 진행되어 오고 있지만 현재 우리가 사용하고 있는 컴퓨터와 같이 universal quantum computer의 개발에 성공하기 까지는 해결해야할 문제들과 한계들이 상당해 보인다. 한편에서는 미래의 양자컴퓨터의 모습은 universal computer로 사용되기 보다는 양자컴퓨팅이 우위를 차지하고 있는 여러 분야에서의 계산상의 우월성을 제공하는 가속기로써 자리매김을 할 것이라는 전망도 있는 것이 사실이다. 그러나, 분명한 것은 만약 universal quantum computer의 형태가 아니더라 로 소인수분해 문제와 이산대수 문제를 풀어주는 전용 양자컴퓨터의 개발의 위협은 여전하므로, 양자컴퓨터 이후 시대의 안전한 통신과 정보보호를 위해 양자내성암호의 개발과 검증은 계속되어야 하며 검증이 완료된 후에는 우선순위 별로 전환을 시작하여 양자컴퓨터 개발이 완료되기 전에 완전한 전환이 이루어져야 한다.

참 고 문 헌

[1] P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring", in Proc. 35th Annual Symposium on Foundations of Computer Science, Santa Fe: NM, pp. 124-134, Nov 1994.

[2] F. Arute, K. Arya, R. Babbush, et al., "Quantum supremacy using a programmable superconducting processor", Nature, vol 574, no 7779, pp.505-510, Oct 2019.

[3] L. K. Grover, "A fast quantum mechanical algorithm for database search", in Proc. 28th Annual ACM Symposium on Theory of Computing, Philadelphia: PA, pp. 212-219, May 1996.

[4] C. Dods, N. P. Smart, M. Stam, "Hash based digital signature schemes", in Proc. 10th IMA International Conference on Cryptography and Coding, Cirencester, UK, pp. 96-115, Dec 2005.

[5] J. Ding, B. Y. Yang, "Multivariate public key cryptography", in "Post-Quantum Cryptography", 1판,

Springer, pp. 193-241, 2009.
[6] D. Micciancio, "Lattice-Based Cryptography," in Post-Quantum Cryptography, 1판, Springer, pp. 147-192, 2009.
[7] R. J. McEliece, "A Public-Key Cryptosystem Based on Algebraic Coding Theory", DSN Progress Report. vol. 44, pp. 114-116, 1978.
[8] A. Rostovtsev, A. Stolbunov, "Public-Key Cryptosystem Based on Isogenies" [Internet], Available: https://eprint.iacr.org/2006/145.pdf, 2021.8.30.
[9] J. Ding and D. Schmidt,"Rainbow, a New Multivariable Polynomial Signature Scheme", ACNS 2005, LNCS 3531, pp. 164-175, 2005.
[10] W. Beullens, "Improved Attacks on UOV and Rainbow", EUROCRYPT 2021, Part I, LNCS 12696, pp. 348-373, 2021.
[11] W. Beullens, "Breaking Rainbow Takes a Weekend on a Laptop", CRYPTO 2022, Part II, LNCS 13508, pp. 464-479, 2022.
[12] W. Castryck and T. Decru, "An efficient key recovery attack on SIDH (preliminary version)", Cryptology ePrint Archive, Paper 2022/975.
[13] D. Robert, "Breaking SIDH in polynomial time", Cryptology ePrint Archive, Paper 2022/1038.
[14] National Institute of Standards and Technology, Round 4 Submissions [Internet], Available: https://csrc.nist.gov/projects/post-quantum-cryptography/round-4-submissions, 2021.8.30.
[15] RFC 8391, "XMSS: eXtended Merkle signature scheme", Internet Research Task Force, 2018.
[16] D. A. Cooper, D. C. Apon, Q. H. Dang, et al., "Recommendation for stateful hash-based signature schemes", National Institute of Standards and Technology, Gaithersburg, MD, SP 800-208, 2020.
[17] RFC 8554, "Leighton-Micali hash-based signatures", Internet Research Task Force, 2019.
[18] TTAK.KO-12.0348-Part2, 다변수 이차식 기반 양자내성암호 - 제2부: HiMQ, 부가형 전자서명 알고리즘, 한국정보통신기술협회, 2020.
[19] TTAK.KO-12.0349-Part2격자 기반 양자내성암호 - 제2부: 링-리자드(Ring-Lizard) 알고리즘, 한국정보통신기술협회, 2019.
[20] D. Moody, The Ship has Sailed: The NIST Post-Quantum Cryptography "Competition" [Internet], Available: https://csrc.nist.gov/CSRC/media//Projects/Post-Quantum-Cryptography/documents/asiacrypt-2017-moody-pqc.pdf, 2021.8.30.

약 력

심 경 아

1992년 이화여자대학교 이학사
1994년 이화여자대학교 이학석사
1999년 이화여자대학교 이학박사
2000년~2004년 한국인터넷진흥원 암호기술팀 선임연구원
2004년~2008년 이화여자대학교 수학과 연구교수
2008년~현재 국가수리과학연구소 공공기반연구본부 본부장
관심분야: 공개키 암호, 양자내성암호, 암호 프로토콜, 블록체인