# 양자컴퓨터 위협 대응을 위한 양자내성암호와 양자암호

**권대성** ISOIEC 암호그룹(JTC 1/SC 27/WG 2) 한국 그룹장, 국가보안기술연구소 연구위원

## 1. 머리말

최근 AI가 거의 모든 ICT와 결합되며 디지털 대전환이 일어나는 가운데, 다양하게 생성·유통되는 데이터의 보호, 자동화된 기기의 제어 안전성 확보, 개인정보 보호의 필요성이 증가하고 있다. 이를 위한 가장 중요한 기반이 암호 기술이다. 암호 기술은 고대로부터 우리 생활의 안전과 매우 밀접한 관계가 있었다. 현대에 들어와서는 해독 기술의 발전 및 성능 요구조건의 고도화로 인해 안전하면서도 성능이 좋은 암호 기술의 개발은 매우 어렵고 도전적인 과제가 되었다.

역사적으로 보면, 암호 기술의 1차 변혁은 컴퓨터의 등장이다. 2차 세계대전 때 독일 에니그마(Enigma) 암호를 해독하기 위해 컴퓨터를 활용했다. 여기에 알렌 튜링(Alan Turing)이 큰 역할을 한 것은 잘 알려져 있으며[1], 튜링 어워드(Turing award)는 지금도 컴퓨팅 분야의 노벨상으로 자리매김하고 있다. 컴퓨터에 의하여 기존 암호 기술들이 깨지면서, 컴퓨터에 의한 공격에 안전한 암호를 만들기 위한 시도가 이어졌는데, 이게 현재의 암호 기술이라고 할 수 있다. 현대 암호는 컴퓨터에 의한 공격에 안전하면서도, 다양한 컴퓨팅 프로세스에 탑재되어 잘 동작하는 것을 목표로 발전되어왔다.

현대 암호 기술의 활용성은 인터넷 보급과 함께 더욱 강화되었다. 복잡한 수학적 난제를 기반으로 탄생한 공개키암호는 인터넷 보안 강화에 큰 역할을 하였다. 공개키암호 덕분에 인터넷에서 전자상거래를 비롯, 다양한 경제활동이나 중요한 데이터 전송이 가능해졌다.

그런데 이제 우리는 새로운 커다란 위협을 맞이하였다. 1980년대부터 시작된 양자컴퓨터 연구가 본격화되어 실용화 단계에 접어들고 있기 때문이다.

최근 가장 주목받는 뉴스 중 하나는 2019년 10월 네이처(Nature)에 게재된 구글의 "Quantum supremacy using a programmable superconducting processor"이란 논문[2]과 2020년 12월 사이언스(Science)에 게제된 중국 과학기술대의 "Quantum computational advantage using photons" 논문[3]이다. 이 논문들에서는 초전도체 프로세서 또는 광학 기반 양자컴퓨터가 슈퍼컴퓨터의 계산 능력을 추월하기 시작한 것을 설명한다. 이제 양자컴퓨터의 시대가 바로 눈앞에 다가와 있음을 보여준다. 2020년을 지나며 양자컴퓨터 개발이 가속화되고 있기 때문이다.

양자컴퓨터의 발전에는 긍정적인 부분이 많지만, 현대 암호 체계에는 큰 위협이 되고 있다. 인터넷을 이용한 보안통신, 전자상거래, 블록체인의 주요 보안 기능을 공개키암호가 담당하고 있는데, 양자컴퓨터를 이용하면 현재 주로 사용되고 있는 RSA 등의 공개키암호를 짧은 시간에 깰수 있기 때문이다.

NIST 설문조사에 따르면 전문가들의 의견이 갈리기는 하지만, 현재 가장 많이 사용되고 있는 RSA-2048이 24시간 이내 해독될 가능성에 대해 10~15년 사이에 가능할 것이라는 전망이 우세하다.

이제 암호 기술은 기존 컴퓨터에 대한 안전성 뿐만 아니라 양자컴퓨터에 대한 안전성도 확보해야 하는 시대로 접어들고 있다. 또 암호 해독하는 방법이 지능화되면서 AI와 결합되고 있어, 이에 대한 안전성도 확보해야 하는 상황이다.

양자컴퓨터의 위협이 현실화되면서, 이에 대응하기 위한 기술개발은 두 가지 방향에서 이루어지고 있다.

첫번째는 기존 공개키암호와 같이 수학적 난제를 기반으로 하지만, RSA 암호 등 기존 암호와 달리 양자컴퓨터를 이용한 해독이 어려운 난제를 이용하여 공개키암호를 설계하는 방향이다. 이러한 공개키암호를 양자내성암호(PQC, Post Quantum Cryptography)라고 한다. 이 방향의 연구는 공개키암호가 처음 개발된 1970년대 후반부터 지속적으로 연구가 진행되어 왔다. 양자컴퓨터가 이슈화된 2000년대 초반 연구가 확대되었고, 일부는 실용화도 되었다. 미국 국립표준기술연구소(NIST)는 새로운 우수한 공개키암호를 확보하기 위한 공모사업을 2016년부터 진행하고 있으며, 2024년 표준화를 완료한다는 목표다[4].

두번째는 양자키분배(QKD, Quantum key distribution) 기술이다. 공개키암호가 수학적 문제를 기반으로 만들어졌다면, QKD는 물리적 측면에서 양자역학적 원리를 기반으로 양자를 이용하여 공개키암호의 주요 기능인 키분배를 실현한다. 양자 기술의 활용 측면에서 1980년대에 제안되었고[5], 양자컴퓨터 이론이 발전한 2000년대 초반부터 실용화를 위한 연구 및 개발이 진행되었다. 에드워드 스노든이 2013년 미국 NSA의 도청을 폭로한 이후, 도청에 원천적으로 막을 기술로 주목받으며, 세계 각국에서 투자 및 적용이 확대되고 있다.

두 기술은 모두 양자컴퓨터 위협을 대응하기 위한 암호 기술이라 할 수 있다. 양자내성암호는 현재 양자컴퓨터에 안전한 공개키암호를 지칭하고 있는데, 이는 새로운 기술 분류라기보다는 공개키암호에 대한 새로운 안전성 요구조건이라고 보는 편이 맞을 것 같다. 그리고 현대 암호 전체가 양자컴퓨터에 대한 안전성을 가져야 하므로, 양자내성은 양자컴퓨터로의 전환 시기에만 특징적으로 사용될 것이다. 일정 시간이 지나면 현대암호의 안전성 요구조건 중의 하나로 자리잡는 것이 자연스럽다.

양자암호란 분류는 에너지의 최소량인 양자를 이용한 암호 기술로 정의하는 것이 일반적이다. 양자키분배는 양자암호 중의 하나의 분야이며, 실용화에 근접해 있는 기술이라고 할 수 있다. 양자키분배 뿐만 아니라 암호의 기능인 인증, 전자서명, 비밀분산, 공개키암호 등도 양자 기반으로 개발하는 움직임이 있는데 이를 통칭하여 양자암호라고 분류한다.

본 고에서는 양자컴퓨터의 공개키암호 해독 위협에 대응하기 위한 두 가지 암호 기술에 대해 간단히 설명하고, 관련 표준화 동향을 살펴본다. 2절에서는 양자내성암호, 3절에서는 양자키분배 기술을 설명하고, 표준화 동향을 살펴본다. 4절에서는 두 기술의 비교 및 향후 진행 방향 등에 대하여 정리해본다.

## 2. 양자내성암호

### 2.1 양자내성암호 기술 개발 현황

현재 가장 널리 사용되는 공개키암호로는 DH(Diffie-Hellman) 키 교환, RSA(Rivest-Shamir-Adleman), 타원곡선암호(ECC, Elliptic Curve Cryptography)를 들 수 있다. 이 암호 기술들은 소인수분해 또는 이산 로그 문제라는 수학적 문제의 어려움에 안전성의 기반을 두고 있다. 하지만 양자컴퓨터가 개발되면 소인수분해나 이산 로그 문제는 다항식 시간 내에 해결 가능해지기 때문에 더 이상 난제가 아니게 된다. 그 결과 양자컴퓨터가 개발되면 현재 가장 널리 사용되는 공개키 암호들이 더 이상 안전하지 않게 된다. 이러한 이유로 현재 암호 분야에서는 양자컴퓨터에 안전한 공개키 암호의 개발이 활발하며, 이를 표준화하기 위한 작업이 한창 진행 중이다.

앞서 언급한 양자컴퓨팅에 안전한 공개키 암호는 양자내성암호(PQC)로 부르고 있다. 양자내성암호는 기존 공개키암호인 RSA나 ECC의 연장선에 있다. 기존 공개키 암호는 앞서 언급하였듯이 수학적 난제에 안전성의 기반을 두고 있다. 양자내성암호 역시 수학적 난제에 안전성의 기반을 두고 있다. 단, 기존 공개키 암호의 기반 난제는 양자컴퓨팅을 이용한 다항식 시간 측면에서 효율적인 해결 알고리즘인 'Shor 알고리즘'이 알려져 있는 반면, 양자내성암호는 효율적 해결 알고리즘이 알려져 있지 않은 수학적 난제에 기반을 두고 개발되고 있다.

양자컴퓨터의 실용화에는 아직 많은 시간이 남아 있다고 보이지만, 양자내성암호의 개발 및 표준화는 지금부터 준비해야 한다. 이는 모스카 부등식(Mosca's inequality)에서 보듯이 암호 기술은 개발 후 적용에 걸리는 기간 및 데이터 보호가 필요한 기간을 고려하였을 때, 해독 기술이 본격화되기 수년 전에 미리 개발 및 적용이 완료되어야 하기 때문이다.

양자내성암호에 대한 구체적 논의는 2006년 PQCrypto 학회가 시작되면서 본격화되었다. 그렇지만 기술 개발은 그 이전부터 진행되어 왔다. 1970년대 후반 부호 기반 공개키 암호 McEliece 및 해시함수 기반 Lamport, Merkle 전자서명, 2000년대 초 격자 기반 공개키 암호 NTRU 등이 연구개발되고 있었다. 이 암호들은 양자컴퓨터에 안전성이 강한 해시함수, 격자/부호에서의 에러를 이용한 문제 등을 기반하여 암호를 설계하여, 지수승을 이용하기 때문에 양자컴퓨터를 이용한 병렬계산으로 안전성이 저하되는 기존 RSA의 문제를 피하는 방법을 선택하였다.

이러한 연구개발은 오랫동안 사용되어온 RSA이나 타원곡선암호 등을 대체하기 연구 측면에서 진행이 되었으나, 호환성이 필요한 인프라의 특성상 제한적으로 활용되었다.

2010년 초반 양자컴퓨터 연구에 다양한 진전이 이루어지면서, PQC 연구개발이 본격적으로 활발해졌으며, 최근에는 양자내성암호의 구현 테스트도 다방면으로 이루어지고 있다. 예를 들어, Microsoft는 PKI에 전자서명 Picnic을 구현하였고, 키교환 알고리즘 NewHope는 구글의 인터넷 브라우저 크롬 및 인피니언 비접촉 보안칩에 구현되었다.

### 2.2 NIST의 양자 내성 암호 공모사업

NSA는 2015년 공개키암호를 양자내성암호로 전환하는 계획을 발표하였으며, NIST는 양자컴퓨터 위협에 대응하여 2016년 기존 표준 공개키암호를 대체하기 위한 양자내성암호 공모사업을 시작하였다.

현대 암호는 안전성과 각종 플랫폼에서의 성능을 모두 갖춘 암호를 찾는 것이 목적이며, NIST

공모사업에서는 이와 더불어 기존 암호의 교체용이성, 부채널 공격에 대한 내성 등도 평가 항목에 포함하여 진행하였다.

1라운드 평가대상 접수는 2017년 12월까지 이루어졌는데, 세계적으로 69개의 후보가 제출되었고, 5개는 안전성 문제 등으로 철회되었다. 한국에서도 5개를 학계, 연구소 등이 제출하였다. 후보들은 기반을 두는 문제 특성에 따라, 격자(lattice), 코드(code), 다변수(MQ ), 해시(hash), 기타의 5개로, 기능에 따라 서명, 키교환/암호화 2개로 분류하였다.

기능을 2개로 분류한 것은 공개키암호의 주요 용도에 따른 것이다. 큰 데이터의 암호화보다는 ARIA, AES 등 비밀키 암호의 암호키 교환을 위한 연산(KEM, Key Encapsulation Mechanism), 메시지/사용자 인증 및 부인 방지를 위한 전자서명(Digital Signature)이 주요 용도이기 때문이다.

학계의 검증, 공개 워크숍 등을 통해 1라운드 후보들에 대한 평가가 진행되었는데, 주로 안전성 관점에서 진행되었고, 2019년 1월 26개의 2라운드 후보를 선정하였다. 한국에서 제안한 5개의 알고리즘은 2라운드 후보에 선정되지 못했다. 아시아에서는 중국이 제안한 1개 후보만 2라운드 후보에 포함되었고, 미국, 프랑스, 네덜란드 제안알고리즘들이 주를 이루었다. 1라운드 과정에서 약 25개 알고리즘이 해독되거나 취약성이 발견되었다.

2019년 1월부터 시작된 2라운드에서는 안전성과 더불어 성능평가가 이루어졌는데, 이 과정에서 7개의 알고리즘이 추가적으로 해독되거나 취약성이 발견되었다. 복잡성이 검증된 기반문제로부터 만들어졌다고 해도 기반문제로부터 암호화함수를 만드는 과정이 완벽한 안전성을 제공하지 않으므로, 이에 대한 다양한 공격방법이 지속적으로 도출되고 적용되는 것이 현대 암호의 특징이다. 그리고 이러한 분석은 대상을 좁혀 집중적으로 진행하여야 심층 분석이 가능하기 때문에, 여러 라운드를 거쳐 대상을 좁히는 방식을 택하고 있다. 또 대상 선정에는 성능도 고려되는데, 낮은 성능의 암호는 적용에서 후순위로 밀릴 수 밖에 없기 때문이다. 2020년 7월 3라운드 대상을 발표하였는데, 7개 최종 후보와 8개의 대안 후보를 발표하였다. 최종 후보와 대안 후보로 나눈 것은 다른 공격 방법으로 최종 후보들에 문제가 발생할 수 있다는 점과 이를 고려하여 안전성 및 성능에서 다양성을 확보하고자 하기 한 것이다. 3라운드에서는 주로 격자기반 암호들 중심으로 선정된 것을 볼 수 있다. 격자 기반 암호들이 안전성이나 성능 면에서 다른 기반 암호들보다 장점을 가진다는 점을 보여주는 결과라고 해석할 수 있다.

3라운드에서는 양자 및 고전 안전성, 다양한 플랫폼에서의 성능, 부채널 공격에 대한 안전성 등이 중점 항목이 되었는데, 이는 기본적인 안전성 외에 제안되는 양자내성암호들의 키/서명 크기가 크다는 것과, 양자내성암호들은 복잡한 연산을 사용하므로 많은 부채널 공격이 가능하다는 경험을 고려한 것으로 볼 수 있다.

진행하는 과정에서도 2라운드에 걸친 안전성 분석이 진행되었지만, 3라운드 후보에 대하여 기존에 발견하지 못한 취약점이 발견되기도 하였다. 3라운드를 2년 가까이 진행한 후, 2022년 7월 4개의 선정 암호를 발표하였다.

키교환/암호화에 CRYSTALS-Kyber 1종, 전자서명에 CRYSTALS-Dilithium, Falcon, SPHINCS+ 3종을 선정하고, 추가 선정을 위한 4라운드 후보로 키교환/암호화에 ClassicalMcEliese, BIKE, HQC, SIKE 등 4종을 포함하고, 전자서명은 추가 공모사업을 진행하는 것을 발표하였다.

키교환의 CRYSTA LS-Kyber, 전자서명의 CRYSTALS-Dilithium, Falcon이 격자기반 암호들이다.

SPHINCS+의 경우 당초 대안 후보였지만 선정되었는데, 이는 해시함수 기반 서명이 다른 기반 문제들보다는 안전성에서 장점이 있다는 점이 고려되었다고 볼 수 있다.
전자서명 분야에서는 추가 공모사업을 진행하기로 한 것은 기존 선정된 암호들이 다양한 환경, 특히 경량 환경에 대한 적용성이 낮았기 때문이다. 다양한 환경에 적용 가능한 새로운 암호 선정을 추진하는 것을 선택했다. 기존 선정된 암호들이 주로 격자기반이기 때문에, 다양성 측면에서 격자가 아닌 전자서명 방식 선정을 목표로 하고 있으며, 공모사업 4라운드와는 별개로 진행할 예정이다.
NIST 양자내성암호 공모사업의 가장 큰 의미는 암호분야의 세계 각국의 역량을 집결하여, 양자컴퓨터 위협에 안전한 공개키암호 연구를 진행하여, 대표적인 기술을 확보하는 계기가 되었다고 볼 수 있다. 한편에서는 현재 기술은 키/서명 크기 등에서 다양한 환경 활용에 제한이 있기 때문에, 아직은 양자컴퓨터가 나오지 않아 이를 위한 연구도 지속되어야 한다고 언급하고 있다.

### 2.3 양자 내성 암호 적용을 위한 표준화

NIST 공모사업을 통하여 우수한 성능의 양자컴퓨터 위협에 안전한 공개키암호 기술을 확보하였으며, 이제 이를 활용하기 위한 작업이 시작되고 있다.
먼저 안전한 파라미터 등 세부 규격을 확정해야 한다. 상호운용성 있게 하기 적용하기 위한 알고리즘 표준화, 결정된 규격을 각종 응용 프로토콜 및 제품에 적용하기 위한 응용 표준화, 기존 양자컴퓨터 위협에 안전하지 않은 공개키 암호를 대체하기 위한 이전 작업들이 필요하다. NIST에서는 공모사업으로 선정된 암호들에 대하여 2024년까지 표준화를 진행할 계획이다.
암호 분야 가장 영향력 있는 국제 표준화기구인 ISO/IEC에서도 표준화가 진행되고 있다. ISO/IEC에서 암호알고리즘 표준화를 담당하는 ISO/IEC JTC 1/SC 27/WG 2 (정보 보안, 사이버 보안, 개인정보보호 – 암호 및 보안 메커니즘)은 NIST 공모사업 진행 도중, NIST 공모사업에 협력하고 공모사업 이후 표준화를 진행하고자, 양자내성암호에 대한 이해를 돕기 위한 기술 분야별 현황 분석을 담은 공개 기술 문서 SD8(Standing Document 8)를 공개하였다. 기술 분야는 NIST 공모사업과 동일하다.
다만 양자내성암호 기술 중 개발 후 충분한 검증 기간을 가졌던 해시함수 기반 전자서명에 대해서는 우선적인 표준화가 진행되고 있다.
해시함수 기반 전자서명은 2종으로 나뉘는데, 서명할 때마다 서명키를 갱신해야 하는 stateful과 그렇지 않은 stateless 해시함수 기반 전자서명이 있다. Stateful 해시기반 전자서명은 안전성이 해시함수의 안전성에만 의존하기 때문에, 양자컴퓨터에 대한 안전성을 보장하지만 일반적인 목적으로 사용하기에는 한계가 있다. 그렇지만 공모사업이 종료되기 전이거나, 공모사업이 종료되더라도 선정된 암호들에 대한 의문이 있을 경우, 안전성에 대한 신뢰를 가지고 우선 적용할 수 있는 전자서명이다.
Stateful 해시함수기반 전자서명의 대표적 알고리즘으로는 XMSS와 LMS가 있다. 이들의 표준화는 사실 표준화 기구인 IETF(Internet Engineering Task Force)에서 먼저 진행되었으며, 2018년과 2019년 RFC 8931(XMSS)와 RFC 8554(LMS)로 각각 발간되었다.

NIST도 우선 필요한 곳에 적용하기 위하여 2020년 표준(SP 800-208, Recommentation for Stateful Hash-Based Signatute Schemes, 2020, OCT)을 발간하였다. 이 표준은 IETF 표준인 XMSS 및 LMS 외에 다중 트리 버전인 XMSSMT와 HSS를 포함하였다. 이 표준을 통하여 필요할 경우 연방정부 보안에 사전 적용되는 것이 권고되기도 하였다.

대표적 국제표준화 기구인 ISO/IEC에서도 NIST 표준화 이후 표준화가 진행되고 있다.

ISO/IEC의 표준화는 전자서명의 한 부분으로 진행되고 있다. ISO/IEC의 전자서명 프로젝트 번호는 14888(부가형 전자서명, Digital signatures with appendix)이다.

ISO/IEC에서 전자서명은 부가형 전자서명과 복원형 전자서명이 있다. 부가형 전자서명은 기존 메시지 이후에 전자서명 기능을 위한 부가적 정보를 추가하는 형태이고, 복원형 전자서명은 메시지와 부가정보를 별도로 다루지 않고 전자서명 확인 과정에서 메시지를 얻는 방법이다. 주로 사용하는 전자서명 방법은 부가형 전자서명이다.

양자내성 전자서명 표준화는 양자내성을 현대암호가 지녀야 할 특성으로 이해해서 기존 전자서명의 한 부분으로 표준화를 진행하는 추세이다. 국내에서는 양나재성암호를 기존 현대암호와 별도의 기술로 이해하는 경우도 있는데, 이는 올바른 이해가 아니다.

NIST 공모사업 결과 선정된 키교환/암호화, 전자서명의 경우 NIST가 파라미터 사용에 대한 표준화를 먼저 진행한 후 ISO/IEC 표준화를 진행할 것으로 예상된다. 모두 별도 표준 분류가 아닌 기존 표준 분류에 포함하여 표준화가 진행될전망이다.

2022년 ISO/IEC에서는 독일의 제안으로 키교환/암호화 부분에서 NIST가 선정한 CRYSTALS-Kyber와 최종 선정되지 못했지만 공모사업을 통해 안전성이 검증되고, 유럽 등에서 활용성이 있는 Frodo-KEM, Classic McEliece을 추가하여 ISO/IEC 표준화를 추진하는 논의(PWI 19541, Inclusion of key encapsulation mechanisms for Post-Quantum Cryptography in ISO/IEC standards)가 진행되고 있다.

국내에서는 5종의 알고리즘을 NIST 공모사업에 제안하였는데, 2라운드에 포함되지 못하였다. 그 중 2개의 알고리즘 개발자들이 국내 활용을 위하여 TTA 표준화를 진행하였다.

다양한 응용 프로토콜에 대한 표준 확보도 중요한 문제이다. 암호를 암호제품에 적용하기 위한 표준화는 주로 IETF에서 진행되고 있다.

IETF에서 응용프로토콜에 PQC를 적용하기 위하여 진행하고 있는 표준은 다음과 같다.

- Internet X.509 Public Key Infrastructure – Algorithm Identifiers for Kyber, 2022
- Internet X.509 Public Key Infrastructure: Algorithm Identifiers for Dilithium, 2022
- Use of KYBER in the Cryptographic Message Syntax (CMS), 2021
- Related Certificates for Use in Multiple Authentications within a Protocol. 2022
- Hybrid key exchange in TLS 1.3, 2023
- Framework to Integrate Post-quantum Key Exchanges into Internet Key Exchange Protocol Version 2 (IKEv2), 2020
- Beyond 64KB Limit of IKEv2 Payloads, 2023

ISO/IEC 표준 중 인증, 익명성 제공, 부인 봉쇄 등 많은 응용표준들이 RSA 또는 이산로그 문제를 활용하고 있어, 이들을 이용하는 서비스에서 이를 대체하는 표준화 작업이 필요하다. 다음은 ISO/IEC 암호 표준 중에서 수정이 필요한 표준들의 범주이다.
주로 NIST 공모사업 이후에 선정된 암호를 대표적 프로토콜인 TLS, IPsec, 인증서(X.509)에 적용하기 위한 작업들로 볼 수 있다.

2.4 양자 내성 암호로의 전환

양자내성암호 개발 목적이 기존 공개키암호 RSA 등을 대체하기 위한 것이므로, 암호알고리즘을 교체하는 작업을 진행해야 하는데, 이는 단순한 작업은 아니다.

- 기존 제품의 암호를 한꺼번에 교체하는 것은 쉽지 않으며
- 그렇다고 기존 제품을 모두 폐기하고 신규 제품을 도입하는 것도 쉽지 않고
- 암호통신을 하기 위해서는 신규 제품과 기존 제품의 연결을 어느 정도 보장할 수 있어야 한다

이러한 작업은 기존 표준에서부터 진행되고 있다. IETF 표준 등에서는 기존 제품과 일시적으로 호환하면서 신규 선정된 암호를 다중으로 사용하기 위한 규격들을 우선 적용하고 있다.
기본으로 기존 기술 사용을 한시적으로 허용하면서, 신규 기술로 전환할 수 있는 표준들이 준비되면 이러한 기술/표준이 제품에 적용되도록 유도하는 정책이 필요하다.
대표적인 것은 NIST가 2021년 8월 발표한 "MIGR ATION TO POST-QUANTUM CRYPTOGRAPHY"이다.
전환 순서로는

- 양자컴퓨터 공격에 안전하지 않은 공개키암호가 포함된 FIPS-140 인증 SW/HW 모듈
- 양자컴퓨터 공격에 안전하지 않은 공개키암호가 포함된 암호 라이브러리
- 양자컴퓨터 공격에 안전하지 않은 공개키암호가 포함하거나 이에 중점을 둔 암호 응용 제품
- 컴퓨팅 플랫폼에 내장된 양자컴퓨터 공격에 안전하지 않은 암호코드
- 양자컴퓨터 공격에 안전하지 않은 암호알고리즘을 사용하는 통신 프로토콜

유럽에서는 2022년부터 양자내성암호로의 전환(Transition towards Quantum-Resistant Cryptography, TOPIC ID: HORIZON-CL3-2022-CS-01-03) 과제를 진행하고 있다.
이 과제의 목적은 다음과 같다.

- 미래에 안전한 암호를 분석, 평가, 표준화, 인증
- 양자컴퓨터에 안전한 암호의 이론적인 가능성과 실제적인 구현에 대한 차이 도출
- 양자컴퓨터에 안전한 암호학적 프리미티브와 프로토콜을 보안 솔루션에 구현
- 현대 암호에서 미래에도 안전한 암호로의 전환에 필요한 솔루션 및 방법
- 대형 스케일의 양자컴퓨터 공격에도 안전한 정보 교환 및 처리에 대한 준비도

프랑스 ANSSI는 3단계로 전환에 대하여 이야기 하고 있다.

- 단계 1은 양자내성암호 전환에 대한 준비 단계로 양자내성 암호의 안전성에 집중해야 하는 단계. NIST 공모사업 선정결과와 공모사업에 최종 선정되지 못했지만 충분한 안전성이 검증된 암호알고리즘들을 대상으로 선정
- 단계 2는 양자내성암호들에 대한 좀 더 엄격한 제한과 양자내성 안전성을 제공하지 않는 제품들의 조달을 점진적으로 중단
- 단계 3에서는 특정 양자내성암호는 다른 암호들과 결합되지 않고 사용되어야 하고, 양자내성 안전성이 기본 특성으로 설정

양자내성암호 개발 및 표준화의 남아 있는 숙제는 '양자컴퓨터에 대한 안전성을 어떻게 검증해야 하는가?'이다. 이는 물론 아직 고성능의 양자컴퓨터가 개발되지 않았기 때문이다. 양자내성암호의 안전성 기반이 되는 수학적 난제들을 해결할 수 있는 양자 알고리즘에 대한 연구와 더불어 최근 연구되고 있는 양자 인공지능을 이용한 문제 해결 연구 등에 더 많은 연구와 시간이 필요하다는 시각도 존재한다.

## 3. 양자키분배

### 3.1 양자키분배 기술

양자컴퓨터 위협에 대하여 또 하나의 방안으로 제시되는 것이 양자통신을 이용하여 공개키암호의 주요 기능 중 하나인 암호키를 분배하는 기술이다. 이러한 기술을 양자키분배(QKD)라고 한다.

양자통신은 원자, 중성자, 전자, 광자 등 에너지의 최소 단위인 양자를 이용한 통신 기술이다. 양자통신은 양자역학 법칙에 의하여 데이터를 보호할 수 있는 장점을 가지고 있다. 광케이블을 따라 광자에 데이터가 실려 전송될 때, 광자들은 0과1의 중첩(superposition) 상태가 되는데, 이러한 광자를 양자 비트(Quantum bit) 또는 큐빗(Qubit)이라고 한다, 해커가 전송되는 큐빗을 관찰하려고 하면, 상태가 0 또는 1로 결정되고 원래 상태로 복구가 불가능하다. 이 성질은 해커가 흔적 없이 도청을 할 수 없다는 것을 의미한다. 이런 성질로 인하여, 강대국의 정보수집이 광범위하게 일어나고 있는 상황에서 도청에 원천적으로 안전한 양자통신은 중요한 역할을 할 수 있다.

양자통신이 도청에 강한 특성을 가지고 있지만, 양자통신을 이용하여 두 사용자가 안전하게 암호키를 도출하는 과정에 대해서는, 중간에 정보가 노출되지 않는다는 보장할 수 있는 정확한 절차가 필요하다. 1984년 C. Bennett과 G. Brassard가 양자물리학에 기반하여 제안한 BB84 양자 기반 암호키분배 프로토콜[5]이 이같은 연구의 시작이라 할 수 있다.

이 방식은 빛이 파동과 입자 두 가지 성질을 모두 가지며, 송신자가 파동의 편광 및 위상은 결정하여 전송할 수 있지만 결정 방식을 알 수 없는 도청자를 비롯한 제3자는 사전에 결정된 정보를 알아낼 수 없음을 양자역학적 원리로 보장한다.

이 방식은 단일 광자를 이용, 두 사용자가 암호키를 도청자에 어떠한 정보를 노출하지 않고 얻을 수 있는 방식이다. 기존 현대암호와 달리 컴퓨팅의 발전이나 기반 문제의 복잡도에 의존하지 않기 때문에 매우 안전한 암호키 분배 방식이다.

현대 암호는 컴퓨터의 계산 능력과 문제를 해결하는 알고리즘에 의존하기 때문에 컴퓨팅 능력 또는 문제 해결 알고리즘의 발전에 따라 안전성에 변화가 발생한다. 그래서 기술 변화에 따른 정기적인 안전성 재검토 및 암호 알고리즘 교체가 필요하다. 적용된 암호 기술의 교체에는 상당한 비용과 복잡한 절차가 수반되며, 교체가 어려운 환경에서는 취약점을 안고 사용을 감수해야하는 경우도 존재한다. 대표적 경우가 앞서 살펴보았던 양자내성암호의 개발 및 전환 절차라고 할 수 있다.

이에 비하여 양자키분배는 컴퓨터의 계산 능력 및 컴퓨터를 활용한 문제해결 알고리즘 능력의 발전과 무관하기 때문에 현대암호의 안정성 문제를 해소하고, 장기간 사용하여도 안전성이 낮아지지 않는 장점을 가지고 있다.

반면, 양자키분배 구현에는 다음과 같은 문제가 있다.

1) 송신부 비용: 단일 광자를 이용한 구현은 난이도가 높으며 많은 비용 필요
2) 거리 한계: 단일 광자는 전송할 때 변형, 소실 등이 발생
3) 양자중계 어려움: 양자를 중계할 수 있는 기술의 부족

2000년대 초반부터 BB84 프로토콜 실용화를 위하여 단일 광자 대신 레이저를 이용하는 방법들이 고안되었다. 레이저를 사용하면 단일 광자를 만들기 어려워 한 번에 여러 개의 광자가 나오게 되는데, 공격자가 일부를 가져가 정보를 탈취하는 방법들이 있다. 레이저를 사용하려면 이러한 공격을 막아야 하는데, 대표적인 방법이 미끼(decoy)를 사용하는 방식이다. 한국인 물리학자 황원영 교수 등이 2003년~2005년 경 제안하였고[6], 2006년 실험에 성공하였다[7]. 이 즈음 산업체에서도 양자키분배 장치들을 출시하여 시험에 접어들었다. 2003년 미국 MagicQ, 2004년 스위스 IDQ, 2008년 Toshiba 유럽 등이 상용 제품을 출시하였으며, 스위스에서는 2007년 IDQ의 양자키분배 장치를 제네바 지역투표에 활용하기도 하였다.

현재 BB84 프로토콜 중심의 다양한 제품 개발 및 시험이 진행되고 있다. 국내 SKT와 KT를 비롯하여, 해외에서는 스위스 IDQ를 시작으로 MagiQ Technologies, Inc.(미국), QNu Labs(인도), QuintessenceLabs(호주), QRate(러시아), SeQureNet(프랑스) 등이 상업적 QKD를 시장에 선보였

으며, 도시바(유럽), 미쯔비시, NEC, NTT(일본) 기업 등이 상용화를 진행 중이다.
거리 문제를 해결하기 위해서 기존 네트워크에 거리가 짧은 양자키분배 디바이스들을 연결하는 양자키분배 네트워크(QKDN, QKD Network) 구조에 대한 연구도 활발하며, 양자키분배 기술을 도입한 통신사들 중심으로 표준화 등이 진행되고 있다.
이와 더불어 기존 양자키분배의 단점을 극복하고자 하는 새로운 방식의 연구 개발도 진행되고 있다. 양자키분배 시스템에 대한 양자적 부채널 공격 등의 가능성이 보고되면서, 이를 원천적으로 방어할 수 있는 측정기기무관 양자키분배(MDI-QKD, Measurement Device Independent QKD) 기술, 키분배 거리를 대폭늘릴 수 있는 트윈 필드 양자키분배(TF-QKD, Twin Field QKD) 기술 등이 속속 등장, 1세대 양자키분배 기술의 한계를 극복하고자 하는 새로운 양자키분배 기술도 활발히 연구되고 있다. 자세한 사항들은 최근 발간된 '2022 양자정보기술백서'에서 정리하여 제공하고 있다[8].
현재는 지상에서 유선 네트워크로 연결하는 구조가 주로 실용화되고 있다. 반면 중국은 2016년 양자통신 전용 위성인 무쯔(Micius)를 시작으로 위성을 이용한 양자위성통신 시대의 개막을 알렸으며, 2021년 통합 양자통신망 구축을 발표하고 지상 700개 이상의 광섬유와 2개의 지3상-위성 링크를 결합한 양자통신 네트워크를 구축하였다.
2019년 9월, 유럽에서는 산학연 총 38개 기관이 참여하여 다양한 모델의 양자키분배 장비를 연결하는 OPENQKD PROJECT를 시작하였다[13]. 이종 QKD 장비를 연결하여 네트워크를 구성하고 안전한 통신을 구현함으로 효용성을 검증 및 증명하고 최종적으로는 유럽 대륙에 양자키분배 네트워크를 구성하는 것이 목표다.

### 3.2 양자키분배 기술 활용을 위한 표준화

양자키분배가 일반적으로 사용되기 위해서는 각종 표준화가 수반되어야 한다. 표준화는 상호호환성이 목적이므로, 세부 요소들에 규격화와 연동 방법, 안전성 관련 요구조건 등이 표준화되어야 한다. 아직도 기술개발이 진행 중이나, 산업화도 함께 진행되고 있어 이를 위한 표준화가 진행되고 있다.
가장 앞서 이에 대한 표준화 작업을 진행한 것은 유럽 표준협회인 ETSI 유럽전기통신표준협회(European Telecommunications Standards Institute)이다. ETSI는 양자키분배 위원회를 두고 있으며, 9개의 GS(Group Specification)와 2개의 GR(Group Report)을 출판하고 갱신하고 있다. 이 표준들은 정식 표준들은 아니다.
국제표준화 기구인 ITU-T에서는 주로 네트워크 관점에서 양자키분배 표준화가 진행되었다. 네트워크 구조 및 네트워크의 보안 요구사항이 주요 사항이다. 양자키분배 네트워크의 인터페이스에 관한 사항은 SG 11(Signalling requirements, protocols, test specifications and combating counterfeit products)에서 표준화가 진행되었는데, 자세한 언급은 생략한다. 양자키분배 네트워크 구조는 SG 13(Future Network)에서 2019년부터 진행되었고, 네트워크 보안 요구사항은 SG 17(Security)에서 2020년부터 표준화가 진행되었다.
상기 표에 제시된 표준은 표준화가 완료된 표준 목록이다. SG13과 SG17에서 다수의 양자키분배 관련 표준화가 진행되고 있다. 네트워크 관점의 표준화는 양자키분배에 국한되지 않고 일반

적인 양자통신으로 확대될 수 있는 표준들이 다수 존재한다. 양자키분배는 송수신 시스템과 네트워크로 구성되는데, 보안 측면의 요소들은 송/수신 시스템과 연관이 많아 상기 표준들은 양자키분배를 보안 측면에서 활용하는 것과는 다소 거리가 있다.

3.3 양자키분배 기술의 보안 영역 활용

양자키분배를 구성하고 있는 양자 소자 기술 및 양자 통신 기술이 계속 발전하고 있어, 당초 적용 분야인 보안 분야도 시험 단계를 지나 본격 적용을 앞두고 있다.

그런데 NSA는 다음과 같은 5가지를 양자키분배의 기술적 한계로 제시하며 도입을 미루고 있다[9].

1. 부분적인 솔루션: 인증/암호화는 현대 암호가 제공
2. 특별한 목적의 장치 필요: 전용 선로 또는 대기 중 전송 장치 필요
3. 인프라 비용 및 내부 위협 증가: 현재는 신뢰 노드 필요 등
4. 이론적 안전성이 아닌 구현물에 대한 안전성 확보 및 검증 필요
5. 서비스 거부 공격 위협 증가: 양자의 민감성에 기인

기존 양자 관점에서 이러한 것들은 보안 분야에 활용하기 위해서 필요한 요소이기도 하다. 양자키분배도 이론적으로는 도청에 대한 절대적 안전성을 제공하지만, 구현에 있어서 각종 소자가 상황에 맞게 제대로 동작하는지, 구현물을 통하여 추가적인 정보가 노출되지는 않는지, 어떤 조그마한 빈틈이 있어, 이를 이용한 공격이 나올 수 있을 것인지에 대해서는 기존 보안에서 오랫동안 학습되었던 경험이 적용되기 어려운 부분이기도 하다.

보안 측면에서 제한성이 있으나, 양자키분배 기능은 양자컴퓨터 위협 대응에 좋은 솔루션이므로, 이를 보안에 적용하고자 움직임이 본격화하고 있다. 양자키분배장치 개발과 시범 적용 사업이 국내외적으로 활발히 이루어지고 있다. 이 기술을 보안에 적용하기 위해 구현 안전성을 시험하는 기준 및 방법을 도출하는 연구가 진행 중이며, 이를 기반으로 하는 표준 및 제도 마련도 시작되고 있다.

국내에서는 2018년부터 구체적 준비를 시작하였다. 이를 위하여 양자키분배 안전성 관련 규격 및 보안 요구사항에 대한 표준을 자체 개발하였으며, 유럽 전기통신표준협회인 ETSI의 규격을 도입하면서 TTA 표준으로 제정하였다.

상기 표준 중 양자키분배 시험 검증과 관련된 표준은 2019년 산학연 논의를 거쳐 이루어져 양자 키 분배 보안 요구사항을 세계 최초로 도출하여 TTA 표준으로 등록하였다.

국제 표준 개발 노력은 ISO/IEC의 JTC 1/SC 27(Information security, cybersecurity and privacy protection)에서 2019년 시작되었다.

표준명은 "ISO/IEC 23837 Security requirements, test and evaluation methods for quantum key distribution"로 다음과 같은 2개의 파트로 나뉘어 있다.

Part 1은 양자키분배의 안전성을 중심으로 하는 요구사항에 대한 것이고, Part 2는 요구사항을

평가/시험하기 위한 방법을 서술하고 있다.
이 표준은 현재 ISO/IEC 표준 절차로 볼 때 출판 직전 단계에 있으며, 조만간 출판이 될 전망이다.
유럽 전기통신표준협회 ETSI는 CC 평가에 활용하기 위한 양자키분배의 기능과 보증요구사항을 정의하기 위한 보호프로파일(PP, Protection Profile) "Quantum Key Distribution (QKD): Common Criteria Protection Profile Pair of Prepare and Measure Quantum Key Distribution Module" 작업을 2019년부터 진행하고 있다. 현재는 v0.8.3이 만들어진 단계이다.
ISO/IEC 및 ETSI의 양자키분배 시험평가 기준은 기존 보안제품의 시험평가에 활용되어 온 국제공통평가기준(CC, Common Criteria, ISO/IEC 15408)에 맞추어 개발되고 있다. 공통평가기준은 보안 문제에 대한 인증을 하기 위한 표준이다. ISO/IEC의 양자키분배 시험평가 표준인 23837은 공통평가기준 표준인 15408을 충분한 안전성을 평가할 수 있도록 보완하는 방향이라면, ETSI의 PP는 공통평가기준 표준인 15408에 맞추어 보호프로파일(PP)를 만들고 있어서 향후 조정이 필요할 것으로 보인다.

국내에서는 2020년부터 정부 주도 시범사업의 양자키분배에 참여한 SKT와 KT 장비를 대상으로 시범검증을 수행하면서 국가용 보안요구사항을 도출하는 작업을 진행하였다. 2022년 6월 정부부처에서는 시범검증 결과를 기반으로 양자키관리장비, 양자키분배장비, 양자통신암호화장비 3종에 대한 국가용 보안요구사항(안)을 발표하였다.
이 중 핵심은 양자키분배장비 보안 요구사항이며, 다음과 같은 항목들이 포함되어 있다.

- 양자 비밀키 관리: 양자키분배 장치를 이용한 비밀키 생성 및 저장 등
- 광학계 및 후처리: 난수생성기능, 광학계 기능, 후처리 기능 등
- 식별 및 인증: 양자키분배 장치에 접근하는 관리자에 대한 식별 및 인증 기능
- 보안관리: 인가된 관리자에게 안전하게 보안 관리를 수행할 수 있는 기능 제공
- 전송 데이터 보호: 양자키분배장치 네트워크의 통신상대 간의 전송되는 데이터 보호
- 저장 데이터 보호: 양자키분배장치에 저장되는 데이터 보호

시험 평가와 제도가 마련되어 가고 있지만, 여전히 안전성에 대한 추가적 검토가 충분히 이루어져야 하는 상황이다. 이를 위해 다음과 같은 항목에 대해 연구개발이 필요하다.

- 양자키분배 장치의 광학 모듈 작동방식에 대한 분석을 통한 불완전한 광학계 성능 파악
- 불완전 광학 모듈에 대한 양자 해킹 방법 연구를 통해 취약점에 대한 양자 해킹 대응방법 개발
- 양자키분배 장치 광학계를 개발하여 실제 양자키분배 장치동작 방식의 특징을 이용한 양자 해킹 가능성 확인 및 양자키분배 안전성/신뢰성 실험

- 양자키분배 시스템의 암호 안전성 보장 방법론 개발은 ①양자키분배 시스템의 암호 안전성 시험방법론 개발과 ②시험방법론의 안전성/보안성 확인 및 ③절차의 타당성 검증으로 구성
- 양자키분배 시스템 안전성 분석기술 적용을 위한 안전성 시험도구 설계를 통해 안전성 시험/평가기술 적용된 양자키분배 시험도구 개발
- 양자키분배 시험도구 시나리오 개발 및 광학계 적용 시험 수행

그리고, 이러한 연구 결과를 반영하여 안전성 기준 및 시험방법을 지속적으로 갱신할 필요가 있다.

### 4. 맺음말

본 고에서는 슈퍼컴퓨터의 한계를 넘어서고 있는 양자컴퓨터가 기존 암호 체계에 가할 위협을 해소하기 위한 방안으로 개발되고 있는 양자내성 암호와 양자키분배기술과 관련, 기술 현황과 적용을 위한 표준화 및 이슈를 소개하였다.

현대암호는 절대적인 안전성을 보장하지는 못하기 때문에 일정 기간이 지나면 취약성이 발생하며, 이를 극복할 기술을 개발하여 대체하는 작업이 진행되곤 했다. 이런 측면에서 양자내성암호를 확보하기 위한 NIST 공모사업 현황, 이를 기반으로 하는 표준화 현황 및 기존 공개키 암호를 대체하기 위한 전환 계획을 살펴보았다.

한편, 컴퓨팅 능력 및 알고리즘 해독 능력에 의존하지 않고 양자역학적 원리에 기반하기 때문에 양자컴퓨터 등 컴퓨팅 능력 발전과 무관한 양자키분배 기술 개발 동향과 이를 활용하기 위한 표준화 현황 및 보안 고려사항들을 살펴보았다.

인터넷 개발 보급에 있어 현대암호가 보안을 책임지는 중요한 역할을 수행하였다. 이제 양자통신도 양자컴퓨터, 양자센서 등의 개발과 더불어 양자프로세서들을 연결하는 양자인터넷으로 발전하고 있다. 현재 양자키분배 기술은 가격이 비싸고 대형 장비가 필요하지만, 관련 소자들의 소형화가 이루어지고 있어 과거 컴퓨터가 고가의 대형 장치에서 저렴한 소형 장치로 발전한 흐름을 재현할 것으로 기대된다.

암호 기술은 기존 인터넷뿐 아니라 양자 인터넷에서도 보안의 기반을 제공하는 역할을 해야 한다. 이를 위해서는 기존 인터넷에서 현대암호, 양자인터넷에서는 양자암호가 적절한 솔루션이 될 것이다. 현대암호는 양자컴퓨터에 대한 안전성을 확보해야 하며, 양자암호 분야에서는 양자키 분배 뿐 아니라 양자인증, 양자서명 등 현재 연구되는 다양한 양자기반 암호 기술을 실용화하는 작업이 진행되어야 할 것이다.

유럽 등에서는 두 기술을 상호보완적으로 적용하는 구조에 대한 논의를 활발히 진행하고 있다. 키분배기능만 제공하는 양자키분배 장치들 간 인증 및 네트워크 구성을 위하여 양자내성암호를 적용하는 구조, 주요 간선 망은 양자키분배를 적용하고 지선은 양자내성암호를 적용하는 방식 등이 논의되고 있다.

양자내성암호, 양자암호 모두 아직 기술 개발과 검토가 지속적으로 필요한 분야로, 지속적이고

활발한 상호협력이 요구되는 상황이다.
양자암호 분야에서는 현대암호의 축적된 설계기술과 양자 기술의 결합이 필요하고, 양자내성암호 분야에서는 안전성 분석을 위하여 양자컴퓨팅에 적용될 양자 알고리즘에 대한 연구 협력이 필요하다.
각 분야에 대한 기술 개발이 진행되고 있지만, 이를 결합하는 기술의 개발은 아직 활발하지 않다. 이러한 분야에서 기술개발을 선도할 수 있으면, 이의 활용을 위한 표준화에서도 주도권을 잡아 관련 산업 분야 선도에도 기여할 수 있을 것이다.

※ 본 연구는 과학기술정보통신부 및 정보통신기획평가원의 정보보호핵심원천기술개발사업의 일환으로 수행하였음[1711193524, 국가공공 정보시스템 안전성 및 활용성 제고를 위한 차세대 암호체계 개발].

[참고문헌]
[1] Turing, A. M. "On Computable Numbers, With An Application To The Entscheidungsproblem", Proceedings of the London Mathematical Society, Volume s2-42, Issue 1, 1937, Pages 230-265.
[2] F. Arute 외, Quantum supremacy using a programmable superconducting processor, Nature, vol 574, 2019.
[3] H. Zhong 외, Quantum computational advantage using photons, Science, vol 370, Issue 6523, 2020.
[4] NIST, Post-quantum cryptography, https://csrc.nist.gov/Projects/Post-Quantum-Cryptography.
[5] 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
[6] Hwang, Won-Young. "Quantum Key Distribution with High Loss: Toward Global Secure Communication". Physical Review Letters. 91 (5): 057901, 2003.
[7] Lo, Hoi-Kwong; Ma, Xiongfeng; Chen, Kai. "Decoy State Quantum Key Distribution". Physical Review Letters. American Physical Society (APS). 94 (23): 230504, 2005.
[8] 과학기술정통부, 한국지능정보사회지능원, 미래양자융합포럼, 2022 양자정보기술백서, 2022.
[9] NSA, Quantum Key Distribution(QKD) and Quantum Cryptography(QC), https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/.

※ 출처: TTA 저널 제206호