양자 컴퓨터 상용화 대비 Post-Quantum Cryptography 국제 표준화 동향

유용석 인천대학교 조교수

1. 머리말

디지털 기술의 눈부신 발달로 우리는 더 많고 다양한 정보를 빠른 속도로 처리하고 공유할 수 있게 되었다. 이런 디지털 기술의 발전은 빅데이터와 인공지능 기술 등을 활용한 새로운 제품과 서비스가 가능하게 하였다. 그러나 다른 한편, 복제가 쉽고 빠르다는 디지털 데이터의 속성은 공개를 원하지 않는 특정 정보를 보호하기 위해서는 큰 어려움이 될 수 있다.

디지털 정보를 보호하기 위한 데이터의 암호화 및 서명 기법으로 현재 전 세계적으로 가장 널리 쓰이는 기술은 RSA 알고리즘이다. RSA 알고리즘은 공개키 암호화 알고리즘으로 한 쌍의 비밀키와 공개키를 사용하여 데이터를 암호 및 복호화한다. 개인키로 암호화한 내용은 공개키로만 해독할 수 있다. RSA 알고리즘의 보안성은 소인수분해에 필요한 계산량이 기하급수적으로 크다는 점에 기반한다.

그러나 전통적인 컴퓨터와 근본적으로 다른 원리에 기반한 양자 컴퓨터가 출현하면서 RSA 기반의 공개키 알고리즘의 보안성이 위협을 받고 있다. 본고에서는 양자 컴퓨터의 상용화에 대비한 암호화 기술의 개발 동향과 국제 표준화 동향을 분석한 뒤, 이를 바탕으로 향후 전망 및 대응 전략을 도출하고자 한다.

2. Post-Quantum Cryptography 기술 출현 배경

소인수분해의 어려움에 기반한 RSA 알고리즘은 컴퓨터의 계산 능력이 발전하면서 지속적인 위협을 받아 왔다. 특히 전통적 컴퓨터의 계산과 근본적으로 다른 연산이 가능한 양자컴퓨터의 상용화가 가시화되면서 RSA 알고리즘의 보안성이 크게 위협을 받고 있다. 양자 컴퓨터는 양자의 중첩 원리를 활용하여 한 번에 복수 개의 상태를 표현하고 계산을 수행할 수 있으며, 이런 특수한 성질을 활용하면 소인수분해의 계산 복잡도를 크게 낮출 수 있다.

양자 컴퓨터가 상용화된 이후에도 정보를 안전하게 보호할 수 있는 기술의 필요성이 대두되면서, 관련 기술의 연구와 상용화가 큰 관심을 받고 있다. 보안성을 확보하기 위한 방법으로 크게 두 가지 접근 방법이 존재한다. 첫째, 복제가 근본적으로 불

<표 1> ETSI CYBER-QSC 의장단 현황

직책	소속	이름
Chairman	Approach Infinity, Inc.	Mark Pecen
Vice Chairman	National Cyber Security Centre(U.K.)	Michael Groves
Vice Chairman	Amazon	Matthew Campagna
Technical Officer	ETSI	Sonia Compans

가능한 상태로 정보를 전송 혹은 저장한다. 이 방법의 대표적인 기술로 비밀키를 양자(quantum)의 상태에 실어서 전송 및 수신하는 양자 암호키 분배(Quantum Key Distribution) 기술이 있다. 양자는 더 이상 쪼개지거나 복제할 수 없기 때문에 양자의 상태에 기록된 정보는 근본적으로 도청이 불가능하게 된다.

다른 방법은 기존의 암호화 알고리즘을 개선하거나 혹은 대체할 수 있는 암호화 알고리즘과 시스템을 개발하여 양자 컴퓨터의 위협으로부터 정보를 보호하려는 방법이다. 양자 컴퓨터가 상용화된 이후에도 정보를 암호화하고 전자 서명을 가능하게 하는 새로운 알고리즘들이 활발히 연구되고 있으며, 이런 다양한 알고리즘들을 통틀어 Post-Quantum Cryptography라고 불린다.

3. Post-Quantum Cryptography 국제표준 동향

3.1 유럽의 Post-Quantum Cryptography 표준화 동향

Post-Quantum Cryptography 기술의 국제표준화는 유럽 표준화기구인 ETSI(European Telecommunications Standards Institute)를 중심으로 활발히 진행되고 있다. 유럽의 EC FP6-project Secure Communication based on Quantum Cryptography를 수행하고, 최근 Quantum Menifesto를 선언하는 등 양자암호통신 관련 기술에 대해 적극적인 투자를 지속하고 있다.

그 일환으로 ETSI 산하에 이 기술의 표준화를 담당하는 ETSI QSC Industry Specification Group(ISG)이 설립되었다. ISG는 빠르게 변하는 시장의 요구에 대응하기 위한 제도로서 ETSI 산하의 다른 프로젝트 그룹에 비해 ISG는 생성과 표준화 진행이 상대적으로 빠른 장점이 있다. ISG에서는 Group Specification(GS)과 Group Report(GR)를 작성하여 출판하는데, GS는 강제력은 없지만 유럽 시장 진출에 중요한 요소가 된다. ETSI QSC ISG는 양자 컴퓨터의 위협 분석, Post-Quantum Cryptography의 사용사례 발굴, 연구되고 있는 Post-Quantum Cryptography 프리미티브의 분석 등의 활동을 하며 Group Report를 출판해왔다.

ETSI QSC ISG는 2017년 1월부로 공식 표준기구인 ETSI TC CYBER-QSC로 전환되었다. ISG 활동을 통해 축적한 기술과 표준화 경험을 활용하여 유럽 공식 표준을 제정하기 위해서 활발히 활동하고 있다. 구체적으로 ETSI TC CYBER-QSC의 의장단은 〈표 1〉과 같다. 표준화 회의는 1년에 4번, 주로 ETSI 본부인 프랑스에서 열린다. 매 회의에 30여 명의 회원들이 참석하는 규모의 전문가 집단이다.

3.1.1 완료된 ETSI QSC ISG 표준

ETSI QSC ISG는 2017년 1월 공식 표준 기구인 ETSI TC CYBER-QSC로 재편되기 전까지 1건의 White Paper와 4건의 ETSI Group Report를 출판했다. 현재까지 출판된 표준 문서는 〈표 2〉와 같다.

ETSI QSC GR 001 Quantum-safe algorithmic framework는 양자 컴퓨터를 사용한 공격에도 강인

<표 2> 출판된 QSC White Paper 및 Group Report(GR)

번호	제목	출판연월	내용
White Paper 8	Quantum safe cryptography and security	2015. 6	Post-quantum에 대한 white paper
QSC GR 001	Quantum-safe algorithmic framework	2016. 7	Post-quantum 암호 프리미티브
QSC GR 003	Case studies and deployment scenarios	2017. 2	사용 사례 및 운용환경
QSC GR 004	Quantum-safe threat assessment	2017. 3	사용 사례별 위험 분석
QSC GR 006	Limits to quantum computing applied to symmetric key sizes	2017. 2	대칭키의 보안성 분석

한 암호 프리미티브에 대해 정리한 문서로 다음 5가지의 알고리즘을 다룬다.

① **Lattice-based primitives:** 격자(lattice) 기반 최적화 문제를 활용한 암호화

② **Multivariate primitives:** system of multivariate polynomial equations 기반 암호화

③ **Code-based primitives:** 고효율의 linear code 기반 암호화

④ **Hash-based primitives:** cryptographic hash function을 활용한 암호화

⑤ **Isogeny-based key primitives:** supersingular elliptic curves 기반 암호화

상기 5가지 프리미티브들은 양자 컴퓨터의 출현에도 보안성을 유지할 수 있는 암호화 기법으로 활발히 연구되고 있다. 어느 한 가지 알고리즘이 다른 알고리즘에 비해 뚜렷한 장점이 부각되고 있지는 않으며, 5가지 모두 유력한 Post-Quantum Cryptography 후보 기술로 주목받고 있다.

ETSI QSC GR 003 Use cases and deployment scenarios는 사용 사례 및 운용환경에 대한 표준 문서이다. 이 문서는 다양한 사용 사례에 대해 Post-Quantum Cryptography 기술을 사용한 key establishment와 authentication 절차 및 요구사항을 정리한다. 주요 쟁점 중 한 가지는 현재 통신 네트워크에 널리 쓰이고 있는 TLS 프로토콜에 쓰이고 있는 기존의 암호화 기술들을 어떤 단계를 거쳐 Post-Quantum Cryptography 기술로 교체할 것인가 하는 점이다. 이를 위해서 기존의 암호화 알고리즘을 Post-Quantum Cryptography로 직접 교체할 경우 fragmentation 등의 문제가 발생할 수 있다. 두 가지 기법을 함께 적용할 수 있는 하이브리드 방법이 검토되고 있다. 이런 예로 Quantum safe Hybrid(QSH)를 들 수 있다. 전체 네트워크의 효율을 극대화하기 위해서는 infrastructure 전체에 대한 수정을 해야 한다. 이것은 인터넷과 같이 큰 네트워크에서는 짧은 시간 내에 이루어지기 어려운 일이며, 소규모의 local network에 시도해 볼만한 접근 방법이다. 한편 차세대 통신 환경인 IoT와 5G 상에서의 보안성을 확보하기 위해서는 power consumption과 latency까지 고려하는 최적의 적용 방법을 도출해야 할 것이다.

ETSI QSC GR 004 Quantum-safe threat assessment는 다양한 사용 사례에서의 양자 컴퓨터의 출현에 따른 위협을 구체적으로 분석한다. 기존 TLS 기반의 통신 방법은 양자 컴퓨터의 상용화에 따라 confidentiality와 authentication이 모두 큰 위협을 받고 있다. IKE에 기반한 IPSEC 또한 양자 컴퓨터가 본격적으로 상용화되면 보안성에 치명적인 결함이 생기게 될 것이다. 공개 키로 직접 암호화를 하는 S/MIME 또한 더 이상 안전하지 않게 될 것이다. 디지털 서명의 근간이 되는 PKI 시스템도 보안성이 취약하게 되는데 이것은 기존의 서명 알고리즘의 보안성이 RSA 등의 소인수분해에 근거하기 때문이다.

<표 3> 진행 중인 ETSI CYBER QSC 표준

번호	제목	내용	현재 상태
CYBER-QSC 007	Quantum-safe key exchange	Post-Quanutm 키교환	approved
CYBER-QSC 008	Quantum-safe signatures	Post-Quanutm 서명	start of work
CYBER-QSC 009	Quantum-safe virtual private networks	Post-Quanutm VPN	early draft

ETSI QSC GR 006 Limits to quantum computing applied to symmetric key sizes는 대칭키 암호화 기법이 양자 컴퓨터의 공격에 강인한지를 분석한다. 비대칭키를 사용하는 공개키 기반의 암호화 기법과 달리 대칭키를 사용하는 기법은 상대적으로 더 안전하다. 구체적으로 256bit 이상의 비밀키를 사용하는 AES와 SHA2/SHA3는 2050년까지 나타날 양자 컴퓨터의 공격으로부터 안전하다고 분석되었다.

3.1.2 진행 중인 ETSI TC CYBER-QSC 표준

Post-Quantum Cryptography에 대한 표준을 담당하던 ETSI QSC ISG는 2017년 1월부로 공식 표준기구인 TC CYBER-QSC로 승격되었다. 그리고 2017년 1월에 공식 표준기구로서 첫 회의를 시작하여 1년에 4차례 표준화 회의를 진행하며 활발히 활동하고 있다.

ETSI에서 모든 표준화 활동은 WI(Work Item) 단위로 이루어진다. 각 WI는 Adoption, Start of Work, Early Draft, Stable Draft, Final Draft for Approval, Approval, Publication의 단계에 따라서 표준화가 진행된다. 현재 ETSI CYBER-QSC에서 3건의 신규 표준 문서를 위한 WI가 진행 중이다(〈표 3〉).

CYBER-QSC 007 Quantum-safe key exchange는 Post-Quantum 키교환 기술에 대한 표준으로 Post-Quantum Cryptography 기술의 핵심 표준이 될 것이다. 라포처는 NCSC(영국)의 Michel Groves이다. 해당 WI는 2017년 9월 회의에서 working group approval을 받은 후 다음 달인 2017년 10월 TC Cyber plenary에서 approved for publication 되었다. 따라서 곧 공식 표준문서로 출판될 예정이다.

CYBER-008 Quantum-safe signatures는 양자 컴퓨터의 위협에 강인한 디지털 서명에 대한 표준 제정을 위한 WI로, 라포처는 INRIA(프랑스)의 Perret Ludovic이다. 2017년 2월에 WI로 adoption 되어 start of work 상태이나 아직 이렇다 할 진전은 없는 상황이다.

CYBER-009 Quantum-safe virtual private networks는 Post-Quantum Cryptography 기술을 활용한 VPN 기술에 대판 표준을 준비하는 WI이다. 라포처는 ISARA Corporation(캐나다)의 Mike Brown이다. 이 WI는 2017년 3월 CYBER-QSC 회의에서 WI로 adoption 되어 5월과 9월 회의를 거치며 초안이 구체화되었다. 현재는 early draft 상태이며, 향후 계획은 2018년 3월까지 stable draft를 완성하고 2018년 하반기에 공식 표준으로 출판할 계획이다.

3.2 북미의 Post-Quantum Cryptography 표준화 동향

북미의 표준을 담당하는 NIST는 유럽과는 다소 다른 전략을 취하고 있다. 이전에 AES 암호화 표준을 제정할 때 공모에 의해 선정한 것처럼, Post-Quantum Cryptography 표준 제정을 위해서도 공모를 통해 선정할 계획이다. 2016년에 Post-Quantum Cryptography 기술에 대한 요구사항을 공개하였고, 2017년 11월 30일까지 전 세계의 모든 연구자로부터 제안을 받고 있다. 제안된 암호 기법

들에 대해서 최소 3년 이상의 공개적인 검증을 거친 뒤에 표준으로 선택할 계획이다.

4. 맺음말

본고에서는 양자 컴퓨터의 상용화에 대비한 Post-Quantum Cryptography 기술의 국제 표준화 동향에 대해서 논의하였다. 유럽은 양자 관련 기술에 대한 투자와 표준화에 적극적이다. 유럽의 표준화 기구인 ETSI에 Post-Quantum Cryptography 기술을 담당하던 ETSI QSC ISG가 2017년 공식 표준 기구인 ETSI TC CYBER-QSC로 전환하였고, 관련 기술에 대한 공식 표준화 작업을 진행 중이다. 이에 비해 미국은 Post-Quantum Cryptography 기술에 대한 표준을 공모와 공개적인 검증 과정을 거쳐 최소 3년 이후에 표준화를 진행할 계획이다.

이처럼 Post-Quantum Cryptograpy 기술의 국제 표준화는 유럽과 미국이 서로 다른 접근 방식을 보이지만 그 중요성은 여전하다. 유럽과 미국에서 진행되고 있는 Post-Quantum Cryptography 기술의 표준화 사례를 참고삼아 체계적이고 전략적인 접근이 필요한 시점이다. 아직 특정 알고리즘이 새로운 암호화 표준으로 선정되지는 않았지만, 새로운 기술들의 특성과 표준화 동향을 예의 주시하고 선제적으로 대응할 필요가 있다.

※본 연구는 미래창조과학부 및 정보통신기술진흥센터의 정보통신·방송 연구개발사업의 일환으로 수행하였다[2015-0-00781, 양자암호통신 분야 QKD 기술 표준개발].

[참고문헌]

[1] P. Shor, Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer, SIAM J. Comput., 26(5), 1997, pp. 1484–1509.

[2] D. Lidar, T. Brun, eds., Quantum Error Correction, Cambridge University Press, 2013.

[3] European Telecommunications Standards Institute White Paper No. 8, Quantum Safe Cryptography and Security: An Introduction, Benefits, Enablers and Challenges, June 2015.

[4] ETSI Committee Technical Working Procedures

[5] NIST, AES Competition, http://csrc.nist.gov/archive/aes/.

[6] NIST, Modes Development, http://csrc.nist.gov/groups/ST/toolkit/BCM/modes_development.html

[7] NIST Special Publication(SP) 800-131A Revision 1, Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths, National Institute of Standards and Technology, Gaithersburg, Maryland, November 2015, 23pp.

[8] NIST Special Publication(SP) 800-57 Part 1 Revision 4, Recommendation for Key Management – Part 1: General, National Institute of Standards and Technology, Gaithersburg, Maryland, January 2016,

[주요 용어 풀이]

- 프리미티브: 복잡한 프로그램을 만드는데 사용될 수 있는 가장 기본적인 단위
- 양자정보통신(Quantum Information Communication): 양자정보통신은 양자암호통신이나 양자 컴퓨팅 등 양자 관련 정보통신기술(ICT)을 총칭한다.
- 양자 암호키 분배(QKD, Quantum Key Distribution): 양자암호통신 기술은 양자의 상태에 정보를 실어서 전송하고 수신하는 기술을 말한다. 양자는 쪼개지거나 복제할 수 없기 때문에, 양자의 상태에 기록된 정보는 근본적으로 도청이 불가능하다. 이런 양자암호통신 기술을 활용하여 비밀키를 분배하고 관리하는 기술이 양자암호키분배 기술이다. 양자암호통신을 통해 분배된 비밀키를 사용하여 데이터를 암호화 하면 전송되는 데이터에 대한 도감청을 근본적으로 막을 수 있다.
- Post-Quantum 암호(Post-Quantum Cryptography): 전통적인 컴퓨터뿐만 아니라 양자 컴퓨터의 공격으로부터도 보안성을 유지할 수 있는 암호화 기술