국가경쟁력 확보가 치열한 양자정보통신 기술

김아정(세종대 전자정보통신공학과 교수, akim@sejong.ac.kr)

1. 국가 주도로 박차를 가하는 양자정보통신의 세계 동향

정보선진국의 타국에 대한 감청 이슈가 대두되고, 양자 컴퓨터 실현이 가속화되면서 수학적 복잡성에 근거한 현 보안 알고리즘은 심각한 위협을 받고 있다. 실제로 현세기에는 불가능하리라 보였던 양자 컴퓨터의 실현이 가속화되어 최근 반도체 기반의 상용화 양자 컴퓨터 구현과 양산에 대한 혁신적 성과들이 보고되고 있다. 이는 현재 사용하고 있는 소프트웨어적 보안 시스템을 무력화시키는 심각한 보안 문제의 대두를 의미한다. 이러한 상황 하에 각 국은 국가적 차원에서 획기적 보안 시스템 확립에 총력을 기울이지 않을 수 없다. 이러한 노력의 일환으로 미국과 일본, 중국, 유럽 선진국들은 국가보안법 차원에서 양자 암호 통신과 양자 컴퓨터 개발에 박차를 가하고 있는 중이다. 양자암호통신은 양자역학의 비가역성을 이용하여 절대 보안성을 보장하는 획기적인 보안 시스템이다. 이에 연관되어 상용화 선두 주자인 양자 키분배(QKD) 망은 양자정보통신 분야의 중요기술로써, 각 국가들은 QKD 망 연구와 개발에 대량의 인력과 물적 자원을 투입해오고 있다.

미국은 2012년 이후 보안상의 이유로 양자정보통신 연구를 비공개로 전환하고 관련 제품을 수출 금지 시켰으나, 그 이전에도 방위고등연구계획국(DARPA, Defense Advanced Research Projects Agency) 망을 포설하고 연간 약 1조원을 양자정보통신에 지원하였다. 국가안보국 NSA는 양자 컴퓨터 개발에 약 천억 원을 투자한 바 있으며 미항공우주국 NASA에서는 560km 거리의 양자암호통신 네트워크를 구축하였다. 유럽은 2008년 SECOQC(Secure Communication based on Quantum Cryptography: EC FP6-project) 망을 구축하였고, 스위스의 제네바의 경우 2002년 양자암호통신망 상용화에 이어 2004년부터 인터넷 투표와 정부 보안 시스템, 양자암호를 통한 송금시스템 포함 금융망에 양자 암호망을 이용해오고 있는 등 유럽연합이나 민간 차원의 개발과 지원을 계속해 오고 있다. 특히 중국의 경우, 양자통신망이나 양자 위성에 있어 후발 주자였으나, 국가 주도로 2016년 베이징과 상하이 간 2000km의 양자 통신망을 완성하였고 그 이전에도 국가 정책 결정이나 정부 기밀 안건에 양자 암호망을 이용해 오고 있는 등 최근 공격적인 개발에 앞장서고 있다. 우리나라는 양자통신 개발기술 시험·인증을 지원하기 위한 테스트베드 구축 단계 진입하여 2016년 세계 최초로 상용망에 양자통신 시험망을 적용하였는데, 인력 자원과 지원의 열악한 상황에서 이 성과는 매우 고무적인 것으로 여겨진다.

2. 상용화를 위한 양자정보통신 표준화 작업

표준화는 양자정보통신 상용화 기술 중 하나인 QKD를 중심으로 2008년부터 ETSI(European Telecommunications Standards Institute)에서 진행되고 있다. 빠르게 변하는 시장의 요구에 대응하기 위해 ETSI QKD ISG(Industry Specification Gruop)에서 GS(Group Specification)의 형태로 제정 중에 있다. Toshiba, NTT를 비롯한 유럽과 중국, 캐나다의 기업과 연구소들이 참여하여 표준화가 진행되고 있다. 현재까지 ETSI 표준화에 관련된 문서로는 다음과 같다.

<표 1> 양자통신 관련 ETSI QKD Group Specification

문서번호	제 목	진행사항
QKD 002	Use Cases	Standard
QKD 003	Components and Internal Interfaces	Amendment
QKD 004	Application Interface	Standard
QKD 005	Security Proofs	Standard
QKD 007	QKD Ontology	Early Draft
QKD 008	QKD Module Security Specification	Standard
QKD 010	IS Trojan	Start of Work
QKD 011	Component characterization: characterizing optical components for QKD systems	Standard
QKD 012	QKD Deploy Parameters	Early Draft

현재 QKD 003은 개정 작업이 진행 중이며, 007 Ontology와 Trojan horse에 대비한 보안 구현인 010 IS Trojan, 012 QKD Deploy parameter 등은 표준화 작업 진행 중이다. 우리나라도 SKT와 퀀텀정보통신연구조합을 중심으로 국제 표준화 활동에 참여 중이다. 퀀텀정보통신연구조합은 국내 양자정보통신 진흥을 목적으로 양자정보통신 연구에 관련된 산학연의 컨소시엄으로써 현재 21개의 회원사로 구성되어 있다. 국제 표준 활동 뿐 아니라 이를 기반으로 2015년부터 국내 표준화 활동도 병행하여 양자암호통신 국내 표준 제정을 한국정보통신협회 TTA TG2에서 수행 중이다.

양자통신의 표준화의 최근 주요 이슈는 그 범위를 실용화에 확장시키려는 시도로 볼 수 있다. 국제적으로 양자암호통신에 대해 기존의 암호모듈 검증제도(CMVP, Cryptographic Module Validation Program)의 암호모듈 검증기준과 정보보호제품 공통평가기준(CC, Common Criteria) 급의 기준 정립에 관심을 모으고 있다. 이와 관련해 2017년 10월 ISO/IEC 회의에서 SC 27에 양자암호통신의 표준활동 포함이 논의되었는데 앞으로의 향방이 주목되고 있다. 미국의 양자정보통신 기술 비공개 전환으로 IEEE 사실표준에서의 표준화 추진은 아직 불확실하다.

3. 맺음말

양자정보통신은 앞에서 살펴본 암호통신 뿐 아니라 양자 컴퓨터, 양자 센서 및 양자난수발생기 등의 양자소자 등 신산업의 창출에 있어 그 범위는 예측이 불가능할 정도로 광범위하고 신기술을 통한 비즈니스와 일자리 창출의 규모는 획기적일 것이다. 특히 초연결 환경, 무선 통신에서 보안에 대한 위험성들은 차세대 시스템이 공중망에 진입해 시장이 성장하는데 큰 걸림돌이 될 수 있을 뿐 아니라 국가 보안 차원에서도 위협에 대응하는 절대적 보안에 대한 연구가 어느 때보다 시급한 실정이다. 양자 기술은 이미 세계 주요 국가들 사이에서 21세기 주요 개발 과제로 선정되어 국가경쟁력 확보 차원에서 치열한 양자정보통신기술 경쟁을 벌이고 있다. 신개척지인 양자 기술 개발은 규모나 특성상 국가적 지원이 필수불가결한 분야로써, 중국의 경우 양자정보통신에서 후발 주자이었으나 국가차원의 전폭적 지원에 힘입어 단시간 내에 기술 주도국으로 앞서게 되었다는 것은 우리에게 시사하는 바가 크다. 양자 기술은 기술 진입 장벽이 높고 외국으로부터의 기술 도입이 어려운 만큼, 미래 산업의 준비에 방향성을 잃다가 기술 정보의 종속국, 보안 취약국으로 도태되지 않도록, 정보통신 인프라 보호 및 기술 자급력 제고를 위한 국가적 양자정보통신 기술 개발이 시급한 시점이다.