미-프랑스, 양자 협력 강화 합의

(2022.12.26., 양자정보연구지원센터)

□ 미-프랑스, 양자정보과학 협력 강화 합의

○ 백악관 과학기술정책국(Office of Science and Technology Policy), 미 대표로 양자정보과학(QIS) 및 기술 협력에 관한 공동 성명 서명

- 과학기술 협력에 관한 협정(Agreement on Science and Technology, 2018) 및 과학기술 협력에 관한 공동 성명(Joint Statement on Science and Technology Cooperation, 2021) 기반으로 작성

○ 양자정보과학 어려운 문제 해결 및 'from lab to market' 양자 기술 전환에 필요한 글로벌 시장과 공급망 구축

- 공동 성명서를 통해 생태계 간 연결과 협력 촉진

○ 양자 컴퓨터, 네트워크 및 센서 개발 뿐만 아니라 대규모 컴퓨터가 현재 암호화 프로토콜에 제기할 위험 다룸

- 양국은 양자 컴퓨터 공격으로부터 보호할 암호화 알고리즘에 대한 새로운 표준 연구

○ 프랑스 양자 컴퓨팅 연구 회사 Pascal, 양자 컴퓨팅의 혁신적 잠재력과 양자 공격으로부터 시스템 보호에서 글로벌 협력의 중요성 강조

- Pascal과 시카고 대학, 중성 원자 양자 컴퓨팅에 대한 협력 발표

○ 유용하고 강력한 양자 기술 개발을 위해 과학적, 기술적, 경제적, 조직적 질문에 직면, 상호 보완성 식별하고 파트너와 협력

□ 미-프랑스, Quantum 협력 강화 위한 공동 성명서 서명(11.30.2022)

○ QIST(Quantum Information Science and Technology) 협력에 관한 공동 성명 서명

- 파리(2018, 과학기술 협력에 관한 협정)와 2021년 과학기술협력에 관한 공동성명 포함, 미-프랑스 협력 강화 위한 협정 기반

- 백악관 과학기술정책실(OSTP), 미-프랑스 공동 원칙에 기반한 공동 양자 목표 달성 위해 협력
- 고등 교육 연구부(프), 양자정보과학 및 기술이 프랑스 경제를 크게 변화시킬 것이라는 믿음으로 공동의 목표 향해 노력

○ 미래 양자 컴퓨터 공격으로부터 보호할 새로운 암호화 알고리즘 표준 개발 위해 협력

- 양국의 양자 연구자들을 모으는 공동 워크샵을 통해 과학 협력 형성 촉진에 도움이 될 것으로 동의

○ NIST, 최초 네 가지 양자 저항(Quantum-resistant) 암호화 알고리즘 발표(구조화된 격자 및 해시 함수 기반)

- 개인 정보보호 보안에 위험있는 미래 양자 컴퓨터 공격에 대비·설계된 첫 번째 암호화 도구 그룹 선택, **양자 후(post-quantum) 암호화 표준**의 일부로 2년 후 완성 예상
- 일반 암호화(general encryption, 보안 웹사이트에 액세스 시 사용)의 경우, CRYSTALS-kyber 알고리즘 선택, 비교적 작은 암호화 키와 작업 속도의 장점
- 디지털 서명(digital signatures, 디지털 거래 중 신원 확인, 원격으로 문서 서명 시)의 경우, CRYSTALS-Dilithium, FALCON 및 SPHINCS+(Sphincs plus) 세 가지 알고리즘 선택

(원문)

1. https://www.fedscoop.com/u-s-france-quantum-collaboration/
2. https://www.quantum.gov/the-united-states-and-france-sign-joint-statement-to-enhance-cooperation-on-quantum/
3. https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms