

SKT-SKB, 국제망에 첫 PQC(양자내성암호) 상용화

**- SKB 글로벌 VPN에 PQC 적용…미국∙일본∙싱가폴 등에 전송 테스트 완료**

**- 미 NIST 선정 PQC 최종 후보 알고리즘 적용…글로벌 확장성과 안정성 확보**

**- ‘양자 하이브리드 키조합’ 국제표준화∙개발 완료, 보안기능시험 사전검증 계획**

**- “QKD와 QRNG 이어 PQC 로 양자 기술영역 확대…표준화∙생태계 선도”**

|  |
| --- |
| **엠바고 : 배포 즉시 사용 가능합니다** |

**[2022. 9. 13]**

SKT와 SKB가 국제망 구간에서 양자내성암호(PQC)를 국내 처음 상용화했다.

SK텔레콤(대표이사 사장 유영상, www.sktelecom.com)은 국제망을 이용하는 글로벌VPN(Virtual Private Network∙가상사설망) 네트워크에서 PQC를 상용화했다고 13일 밝혔다.

※ 양자내성암호(PQC∙ Post-Quantum Cryptography) : 양자컴퓨터로도 풀어내는 데 매우 오랜 시간이 걸리는 복잡한 수학적 알고리즘을 사용하는 암호화 방식

※ 글로벌VPN : 퍼블릭 네트워크(인터넷)에 가상의 사설망을 구축해 구내망처럼 사용하는 기술로, 국내와 해외에 각각 떨어져 있는 디바이스를 연결한다

AI서비스 컴퍼니인 SKT는 이번 PQC 상용화를 통해, QKD(양자암호키분배기)와 QRNG(양자난수생성기)에 이어 PQC(양자내성암호)로 양자암호 기술 영역을 확대하고, 효율적으로 보안성을 강화할 수 있게 됐다.

QKD는 물리적인 키 분배장치를 구간마다 설치·운용하는 반면, PQC는 S/W방식으로 구현돼 보안 영역과 편리성 등에서 상호 보완적인 기술로 평가된다.

또 SKT는 이번에 물리적 제약으로 QKD 네트워크를 사용하기 어려운 국제망 구간에서 PQC를 효율적으로 적용할 수 있음을 보여줬다.

SKB는 지난 8월 S/W 업데이트를 통해 PQC-VPN 설치를 완료하고, 미국∙일본∙싱가폴 등 해외에서 네트워크 테스트를 성공적으로 완료했다고 설명했다.

‘PQC-VPN’은 VPN 네트워크의 보안 강화를 위해, PQC 공개키 암호화(PKE∙Public Key Encryption)/키분배(KEM∙Key Encapsulation Mechanism), 전자서명(Signature) 알고리즘을 적용했다.

**※ PQC-VPN 개념도**



특히 ‘PQC-VPN’은 국내에서 처음으로 NIST(미국표준기술연구소)가 선정한 PQC 알고리즘 최종 후보\*인 ‘크리스털 카이버’와 ‘크리스털 딜리슘’을 채택했다.

※ 주요 후보 2종 : 크리스털 카이버(CRYSTALS-KYBER), 크리스털 딜리슘(CRYSTALS-Dilithium)

 추가 후보 2종 : 팔콘(FALCON), 스핑크스(SPHINCS)

‘크리스털 카이버’와 ‘크리스털 딜리슘’ 두 알고리즘은 향후 PQC 글로벌 표준이 될 가능성이 높아 확장성과 안정성이 뛰어나다는 평가다. 또한, ‘PQC-VPN’은 인증 및 키분배 시에 기존 공개키 기반 알고리즘을 PQC알고리즘과 동시에 활용하는 하이브리드 기술을 적용해 안정성을 강화했다.

이와 별개로 SKT는 21년 12월 10Gbps∙100Gbps급 암호모듈에 대한 KCMVP(국정원암호검증모듈) 인증을 국내 최초로 획득한데 이어 ‘양자통신 암호화장비 하이브리드 키조합’ 기술 개발을 완료했다고 밝혔다.

‘양자통신 암호화장비 하이브리드 키조합’ 기술은 기존의 공개키 기반 암호키와 양자키분배방식에서 분배된 양자키를 조합해 기존 암호화 장비의 비밀키로 사용하는 기술로, 양자암호 확산을 위한 핵심 기술영역이다.

이 기술은 2020년부터 과학기술정보통신부와 한국지능정보사회진흥원(NIA)이 주관하는 양자암호통신 인프라 구축 사업을 통해 국정원에서 마련한 보안요구사항에 맞춰 개발됐다.

또 SKT는 국가보안기술연구소(NSR)과 정보통신기술협회(TTA), 전자통신연구원(ETRI) 등과 협력해 보안 및 안전성 시험을 사전 검증할 계획이다. 아울러 23년 정부 및 공공시장에서 보안기능 시험제도에 맞춘 제품을 출시해 양자암호통신 시장을 선도한다는 계획이다.

SKT는 또 8월 22일부터 9월 2일까지 개최된 ITU-T\* 정보보호연구반(SG 17) 회의에서 ‘이기종 QKD망 연동 보안요구사항’을 신규 표준화 과제로 승인 받았다.

※ 국제전기통신연합 전기통신표준화 부문을 뜻하며, 전기통신 관련 세계 최고 국제기구인 ITU의 산하기관으로 통신 분야의 표준을 정함

이번에 승인받은 표준화 방안은 서로 다른 장비 회사의 QKD를 활용할 경우, 양자암호통신망에서 원활히 양자보안 서비스를 제공하기 위한 보안 요구 사항을 담고 있다.

이에 앞서 지난 5월에는 ITU-T SG17에서 제안한  'QKD를 활용한 하이브리드 키 교환 방법'을 최종 승인받은 바 있다. 이는 QKD를 다양한 네트워크 계층에서 활용하기 위한 표준화 작업으로, QKD와 PQC를 연동하기 위한 초석을 마련한 셈이다.

박종관 SK텔레콤 Infra기술 담당은 “QKD(양자암호키분배기)와 QRNG(양자난수생성기)에 이어 PQC(양자내성암호) 상용화를 통해 AI서비스컴퍼니인 SK텔레콤이 양자보안기술 전반을 주도하는 기술력을 보유하게 됐다”며 “앞으로도 양자암호기술을 선도하고 양자산업 활성화에 기여하겠다”고 말했다.

|  |
| --- |
| **※ 사진설명**SK텔레콤은 국제망을 이용하는 글로벌VPN(Virtual Private Network∙가상사설망) 네트워크에서 PQC를 상용화했다고 13일 밝혔다. SKT 연구원들이 국제망에 PQC를 적용하기 위한 연구를 수행하고 있다. |

**▶ 관련문의 : SK텔레콤 PR담당 전략PR팀 박지웅 매니저 (02-6100-3832)**



**※ 양자암호 관련 연구성과 요약**

|  |  |  |
| --- | --- | --- |
| **구분** | **시기** | **주요 내용** |
| **PQC-VPN** | **2022년 9월 상용화** | **국제망을 이용하는 글로벌VPN에서 PQC(양자내성암호) 상용화** |
| **양자통신 암호화장비 하이브리드 키조합** | **2022년 8월 기술개발 완료** | **기존의 공개키 기반 암호키와 양자키분배방식에서 분배된 양자키를 조합해 기존 암호화 장비의 비밀키로 사용하는 기술** |
| **이기종 QKD망 연동 보안요구사항** | **ITU-T SG 17(정보보호연구반회의) 8/22~9/2** | **서로 다른 장비 회사의 QKD를 활용할 경우, 양자암호통신망에서 원활히 양자보안 서비스를 제공하기 위한 보안 요구사항을 신규 표준화 과제로 결정** |