제목: 개방형 양자암호 네트워크 환경 구성을 위한 양자암호 네트워크 표준화 방안

저자: 상의정, 박춘걸

소속: KT 융합기술원

요약: 양자암호키분배(QKD; Quantum Key Distribution)기술은 양자 컴퓨터의 보안 위협에서 안전한 암호통신 기술로서 멀리 떨어진 두 네트워크 노드 간 양자역학의 법칙들을 따르는 대칭형 암호키를 주고 받을 수 있는 기술이다. 그러나 QKD 는 1:1 양 종단에 연결된 장비로부터 양자키를 생성하며 연결거리가 50Km 내외로 기존의 광통신에 비해 짧아 QKD 만으로는 네트워크를 구성하기가 어렵다. 따라서 이러한 QKD 기술을 이용하여 다자간 암호통신을 할 수 있는 양자암호네트워크 상용화 기술개발이 국내외에서 활발히 진행되고 있다.

본 연구는 이러한 QKD 의 특성을 고려하고 장비간 상호운용성을 제공하는 개방형 양자암호 네트워크에서 QKD 기술과 전달 네트워크 (Transport Network) 기술을 결합한 양자암호 전달 네트워크 기능구조를 보인다. 이 기능구조는 전달 네트워크에서 양자암호를 사용함에 있어서 필요한 기능요소, 운영절차, 보안 고려사항 등을 제안하고 있다. 전송 장비와 QKD 장비는 함께 신뢰 공간에 존재할 수 있으며, 기존의 전달 채널에 양자 채널을 함께 수용할 수 있다는 장점이 있다. 이와 같이 양자암호 네트워크는 QKD 와 특성과 관련 서비스를 고려한 형태로 구성할 수 있으며 추가적으로 이를 위한 네트워크 구조, 키 관리 기술, SDN 기술, 인터페이스 등 양자암호 네트워크에 대한 국제 표준화 동향을 알아본다.

Acknowledgements: