

[정보보호] 암호 통신, 패러다임의 변화를 가져올 것인가?

양자암호통신(Quantum Key Distribution)은 "꿈의 보안"으로 불리는 암호 통신이다. 빛의 알갱이에 편광을 이용한 암호 키를 생성하여 보냄으로써 침입자가 발생할 경우 전송자와 수신자 모두 이를 알아내어 새로운 암호키를 생성 및 전송하여 도청을 근본적으로 차단한다. 컴퓨터의 성능 발전으로 인해 현재의 RSA 암호 등과 같이 숫자를 사용한 암호는 도청을 방지하기 위하여 지속적으로 암호화의 bit수를 늘려왔지만, 컴퓨팅 속도의 발전과 양자 컴퓨터 등의 연구는 숫자를 이용한 암호화 체계에 많은 우려를 주고 있다. 이를 극복하기 위해 양자 암호 통신이 제안되고 연구되어 왔고 지금까지의 실험적인 연구에서 벗어나 새로운 단계로 접어들고 있다.

양자암호통신 관련 국내외 표준화 동향

2008년은 양자암호통신을 태동기에서 벗어나게 하는 새로운 해인 듯하다. 지난 7월 독일의 Siemens사는 양자암호통신 Prototype Chip을 개발했다고 발표하고 10월에 비엔나에서 Demonstration을 갖는다고 발표했다. 또한 ETSI는 Industry Specification Group을 통한 표준화를 7월 29일 본격적으로 시작하였다. 우리에게 GSM과 WCDMA로 익숙한 이 단체에서의 양자 암호 통신에 대한 표준화 진행은 향후 EU의 암호 통신뿐만 아니라 세계의 암호 통신을 양자 암호 통신을 기반으로 "꿈의 보안" 네트워크를 만들겠다는 의지로 볼 수 있다. 양자 암호 통신 R&D는 미국, EU, 일본, 호주, 캐나다 등을 비롯 최근에는 싱가포르에 이르기까지 많은 국가의 대기업, 벤처기업, 대학교 및 정책 연구 기관에서 연구해 왔다. 특히 싱가포르는 양자 암호 통신 및 양자 컴퓨터 개발을 위해 싱가포르 국립대에서 매년 200억 원 이상의 예산으로 2007년부터 본격적으로 연구를 시작하고 EU의 과학자들을 데려다 새로운 시장으로의 진입을 위해 노력하고 있다.

국내의 경우 고등과학원, ETRI, 서울대, KAIST 등에서 연구 및 개발을 하고 있으나 경쟁 국가 대비 지원 및 관심이 부족한 상태이다. 하지만 국내의 인적 자원은 어느 국가 못지 않게 경쟁력이 있는 것으로 판단되고 있다. 또한, 국외 한인 과학자들이 미국, EU, 호주 등에서 관련 연구를 진행하며 결과를 배출하고 있다. 국내외 우수한 인적 자원과 정부 및 대기업의 관심과 투자가 필요한 때이다.

국내 표준화 활동에의 제언

"대한민국은 인터넷 강국이다."라는 정의도 해외 각국의 FTTH 도입 등, 적극적 투자에 밀려 1위 자리를 내어주고 있으며 기존의 위치에서도 우리 기술에 의한 수익 창출은 많지 않은 것이 사실이다.

암호통신의 패러다임 변화가 양자 암호 통신으로 옮겨가게 될지는 아직은 누구도 장담할 수 없는 상황이지만 Siemens, HP, 도시바 등의 대기업 및 2억2천만의 가입자를 보유하고 있는 텔레포니카 등 사업자들의 ETSI표준화 참여는 시사하는 바가 크다. WCDMA로 전 세계를

장악한 ETSI가 양자 암호 통신의 글로벌 표준화 및 상용화를 리드하게 될 경우 우리는 다시 한번 우수한 인재를 보유하고도 "남 좋은 일"만 하게 되는 상황을 만들 수 있다. 일반적으로 표준화가 완성이 된 후 3년 정도의 시간에 상용 시장이 활성화 된다고 가정하고, FTTH가 모든 통신의 기본이 되는 때를 예상한다면 시장의 크기는 현재 휴대폰 시장보다 훨씬 큰 시장이 열릴 수 있게 된다. 모든 PC와 서버 및 스위치 장비에 양자 암호 통신 기술이 들어갈 때를 상상하면 시장의 규모는 거대하게 될 것이다.

현재 국내의 상황은 몇몇의 과학자들에 의해서만 연구가 개별적으로 이루어지고 있다. 이를 통합하여 하나의 목표를 잘 선택하여 새로운 시장에서의 기회를 찾기 위해서는 국내에도 TTA 산하 정보보호기반 프로젝트그룹(PG501)에서 관련 연구가 진행되어 시장의 요구사항을 발빠르게 모으고 이 요구 사항을 바탕으로 기술 개발 및 국제 표준화 단체와의 alliance를 통해 Global 표준화에 참여한다면 향후 암호 통신의 패러다임 변화에서 대한민국이 다시 한번 통신 강국의 면모를 보임과 동시에 국외로부터의 수익 창출에 크게 기여할 수 있을 것이다.

곽승환 (SK텔레콤 미래사업단 매니저, kwaksh@sktelecom.com)