특집 04

기존 암호와 양자기술과의 융합을 통한 암호체계의 강화 및 글로벌 리더십 확보

곽승환 (SK텔레콤)

목 차 »

1. 양자암호통신기술의 상용화 경쟁

지난 2000년대 초반부터 세계 각국은 양자암호시스템에 대해 연구 및 개발을 시작해왔다. 스위스의 IDQuantique(이하 IDQ)와 미국의 MagiQ가 상용 시스템을 시장에 출시하였으나, 당시의 열악한 광통신 네트워크의 환경은 이들의 성공을 보장하지 못했다. 결국 MagiQ는 미국 국방부에 몇 대의 양자암호장비를 납품한 이후 현재는 관련 기술의 Patent Troll화 되었고, IDQ 만이 명맥을 유지해왔다. 물론 도시바, NEC 등의 일본 기업들은 연구소 수준의 장비를 계속 개발하고 있었지만, 아직 사용 장비로는 출시하지 않고 있다.

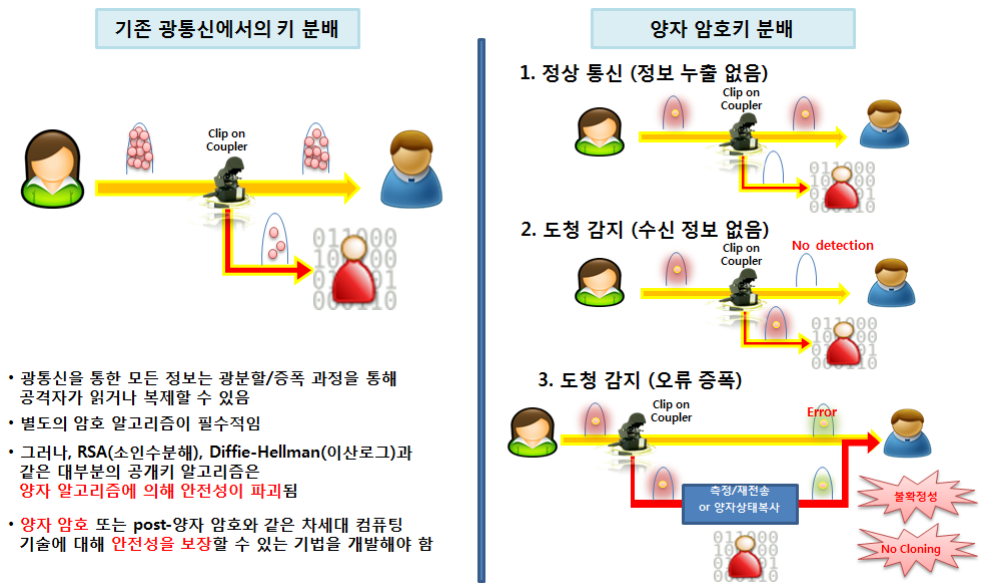
그러나 지난 해 6월 전 CIA직원이었던 에드워드 스노든이 NSA의 세계 각 국가에 대한 무차별적인 도청을 폭로한 이후 양자암호통신기술은 세계적인 주목을 받으며 각 국가의 연구실 차원의 장비들을 상용망으로 끌어내고 있다.

이 문서에서는 양자암호통신기술의 개요, 각 국가의 양자암호통신기술 개발 현황, 향후 방향성 및 새로운 양자기술의 도입을 통한 보안성 강화에 대해 살펴보도록 하겠다.

2. 양자암호통신기술의 개요

양자암호통신에 대해 많은 사람들이 오해하는 것 중에 하나가 데이터 전송을 양자화하여 보낸다고 생각하는 것이다. 양자암호통신을 정확한 이름으로 바꿔 말하면 양자열쇠분배이다. 양자역학으로 설명되는 중첩과 복제불가의 이론을 활용하여 중간에서 도청자에게 열쇠를 도청당하지 않고 완벽하게, “암호화 및 복호화를 위한 열쇠”를 분배하는 기술이다. 또한 이 열쇠는 지속적으로 생성되기 때문에 1분 혹은 그 이하의 시간에 열쇠를 계속 바꿔가며 쓸 수 있다.

그렇다면 통신네트워크를 통한 일반적인 열쇠



(그림 1) 양자암호통신의 도청방지 원리

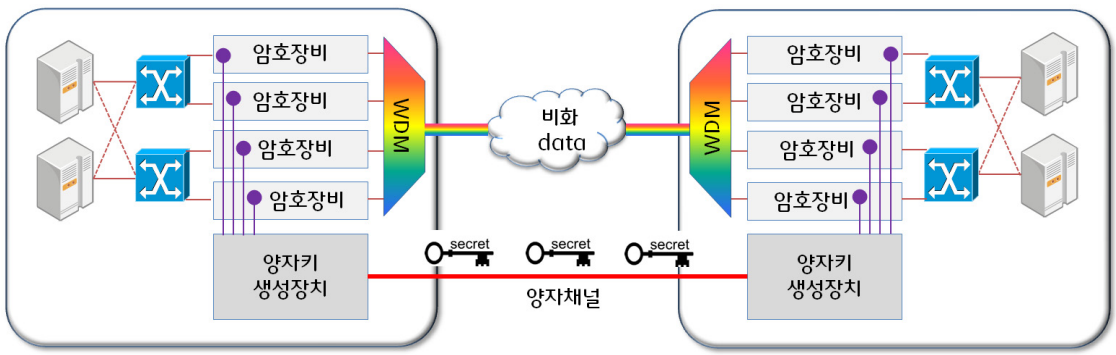
의 분배는 왜 안전하지 않은 것인가? 또한 이 양자기술을 통한 열쇠의 분배는 왜 안전한 것인가?

기존의 광통신 네트워크에서의 신호는 빛이 켜져 있으면 1, 꺼져 있으면 0으로 표현된다. 그러나 이 "빛"은 많게는 9조개 정도의 빛 알갱이로 이루어져있다. 도청자는 이중에 일부만을 빼 내어 증폭하면 기존 광통신 네트워크에서 전송되는 열쇠를 쉽게 알아낼 수 있다. 실제로 지난 부산 World IT Show 2014에서 SK텔레콤은 광통신에서 데이터의 도청을, 단돈 100만원짜리 장비를 구축하여 시연해보였다. (물론 현재 광케이블은 단순한 나선(裸線)으로 이루어져있지 않기 때문에 현재 광통신에서의 도청을 우려할 필요는 없다.)

그러나 양자기술을 통한 열쇠의 분배는 빛 알갱이 하나하나에 편광이나 위상차에 의한 정보를 실어보내기 때문에 일부만을 빼낸다는 것은 불가능하며, 각각의 빛 알갱이가 갖는 중첩 및 복제불가의 원칙이 적용된다. 즉 도청자가 빛 알갱이를 관측할 때, 빛 알갱이는 중첩상태가 붕괴되어 송신자 및 수신자가 도청의 유무를 쉽게 알 수 있다.

이를 통해 만들어진 양단의 암호키는 지속적으로 암호화 및 복호화 장비로 전송되어 데이터의 완벽한 보안을 제공하게 되는 것이다. 이 암호화 및 복호화 장비에서 사용되는 알고리즘은 기존 AES, SEED, ARIA 등의 모든 암호 알고리즘을 동일하게 사용한다.

2000년대 초반 국내의 양자암호기술연구를 막았던 가장 중요한 이유는 이 알고리즘을 연구해왔던 사람들이 양자암호기술이 나오면 본인들의 연구가 필요 없어질 것이라는 "무지"에서 시작된 것이었다. 아마도 양자암호기술의 궁극적인 목표였던 One Time Pad에 대한 우려였을 것이다. 양자암호상용장비를 개발하고 있는 필자는, 특정 채널에 대해서는 소리나 영상 데이터의 One Time Pad는 가능하나 최소 Giga단위로 전송되는 모든 데이터의 One Time Pad 암호화는 향후에도 불가능할 것이라고 판단하고 있으니 기존 암호 알고리즘을 연구하는 분들의 걱정은 기우에 불과한 것이라고 말할 수 있다.



(그림 2) 양자암호시스템의 개요

3. 각 국의 양자암호통신기술 개발 현황

세계 각 국은 양자암호통신기술의 상용화에 박차를 가하고 있다.

미국 정부의 보안 기술 개발에 대한 예산의 제한은 없다. 필자가 지난 8월 참석했던 미국 국회에서 Cloud Computing Caucus Advisory Group 컨퍼런스에서의 슬로건은 매우 인상적이었다. “Security is No.1 Priority in U.S.” 미국은 로스알라모스 연구소는 QKarD 프로젝트를 통해 아주 작은 양자암호트랜시버를 개발하여 몇 개월 전에 Whitewood Encryption systems(이하 Whitewood)로 분사하였다. 이 회사는 이 기술을 통해 Smart Grid, IoT 등에 활용할 것이라고 밝혔다. 또한 Battelle Memorial연구소와 IDQ는 현재 Trust node라는 중계기를 통해 미국 오하이오주에 68km의 거리에서 시범망을 설치하였다.

유럽은 상기한 바와 같이 IDQ로 대표되는 유선망 상용장비 업체와 AIT(Austrian Institute of Technology)로 대표되는 위성을 통한 양자암호통신 기술 개발이 유럽의 양자암호통신기술 개발을 리드하고 있다. 또한 최근에는 위성을 사용하지 않고 태양열만으로 착륙 없이 365일 날아다니는 드론을 통한 양자암호통신기술을 개발 중이다. 특히 LTE기술표준을 주도하고 있는 ETSI(유럽 표준화 단체)는 2008년부터 일찌감치 양자암호기술에 대한 표준화를 준비해오고 있다.

중국은 QuantumCTech. Qasky등의 업체들과 몇군데의 과학기술대학이 협력하여 북경, 상해간 Quantum Backbone프로젝트를 1000억원의 예산을 투입하여 작년 6월부터 구축 중에 있다. 또한 양자암호통신만을 위한 전용 위성을 내후년에 쏘아 올릴 예정이다.

일본은 2000년대 초반부터 양자암호기술을 개발하여 다수의 산업체가 상용화 준비를 하고 있다. 특히 도시바는 지난 5월 British Telecom 및 ADVA와 손잡고 British Telecom의 시험네트워크에서 초당 300kbps의 양자암호키를 생성하여 데이터를 송수신하고 있다. 일본의 가장 큰 고민은 일본의 FTTH가 대부분 전신주를 타고 연결되고 있다는 것이다. 바람에 의한 흔들림과 온도의 변화는 양자암호통신기술에서 가장 큰 영향을 미칠 수 있다. 어쩌면 이 고민이 현재도 그렇지만 향후 세계 최고의 기술을 탄생시키는데 큰 역할을 할 수도 있을 것이다.

우리나라의 양자암호통신기술은 3년 전 까지만 해도 열악했다. 2000년대 초반, 국가보안기술연구소, ETRI, KIST등에서 개발을 시작하였으나 중장기 기술에 대한 우리나라의 인식부족으로 인하여 모든 연구기관에서 연구를 중단하였다. 특

히 ETRI는 2011년 2월에 잘 진행되던 양자암호통신기술을 예산 부족으로 중단함으로써 이쪽 분야의 연구자들에게 절망감을 심어주었다.

그러나 SK텔레콤은 2005년부터 2011년까지 6년에 걸친 준비작업 끝에 그해 10월에 ICT기술원산하에 Quantum Tech. Lab을 설립하여 양자암호통신기술의 새로운 획을 긋기 시작했다. 기술개발이 중단된 ETRI에서의 담당연구원들을 영입하고, KIST에서 개발에 참여했던 연구원도 영입하였으며, 10억원의 KIST투자를 통한 KIST나노양자센터 설립에 기여한 것을 포함 총 23억원의 출연연 및 대학교의 연구비를 지원하였다.

또한 3년간의 개발을 통해 지난 10월20일 부산에서 열린 World IT Show 2014에서 50km에서 10kbps의 양자열쇠생성 및 이 생성된 열쇠를 통해 10Gbps의 데이터를 암호화하여 전송하는 상용시제품의 시연에 성공하였다. 지난 3년간 SK텔레콤이 투자한 비용은 인건비를 포함하여 400억원 정도이다. 향후 이 장비는 행정, 의료, 국방망에 점진적으로 적용되어 나갈 것이다.

정부에서도 미래창조과학부의 출범 이래 양자암호통신기술에 대한 지원을 늘려가고 있다. 초기 3억원에 불과했던 연간지원금이 현재 30억원대로 증가되었으며 내년부터는 총80억원에 가까운 정부지원금이 책정된 것으로 알고 있다. 또한 지속적으로 증가시키겠다는 정부의 의지를 표명하고 있다.

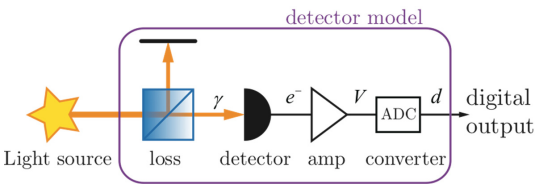
4. 양자암호통신기술의 향후 방향성

양자암호통신기술은 향후 네트워크의 보안기술로써 넓게 확장될 것이다. 지금은 주로 백본망에 적용하는 기술을 전 세계적으로 개발하고 있으나, 국내의 방향성은 사뭇 다르게 가고 있다. 백본망을 위한 기술은 당연히 상용화 될 것이다. 또한 우리나라는 전 세계 최고 수준의 광네트워크를 보유하고 있다. 요즘 신규로 짓는 아파트 및 일반 건물들은 기본적으로 여섯가닥의 광케이블이 연결되어 있다. 이는 정체된 ICT산업발전의 새로운 기회가 될 것이며 우리나라는 양자암호통신기술의 Global Testbed가 될 수 있을 것이다. 특히 SK텔레콤은 다수의 중소기업 및 대학연구소를 지원함으로써 이 분야의 건전한 생태계를 이끌어가고 있다. SK텔레콤 Quantum Tech. Lab은 Quantum To The Home을 지향하고 있다. 아마도 2020년에는 몇군데의 아파트 단지나 건물들은 이 기술을 통해 보다 안전한 통신을 즐길 수 있을 것이다.

5. 새로운 융합보안의 가능성 양자진정난수기술

현재의 암호화 기술은 암호키와 난수를 이용하여 암호화를 진행한다. 이때 사용하는 난수는 진정난수를 사용하여야하나 현재 진정난수 생성기의 비용 및 크기 때문에 대부분 소프트웨어에 기반한 의사난수를 사용하고 있다. 의사난수는 NIST(미국표준연)의 FIPS Level 4으로 지정되어 있다. 그러나 의사난수의 문제점은 일정시간이 지나게 되면 일정한 패턴을 반복하게 된다. NSA는 PRISM을 통해 도청을 해왔는데, 이중 알려진 두 가지 방식은 다음과 같다. 첫 번째는 상기한 대로 백본망에서의 도청, 두 번째는 의사난수의 반복되는 패턴을 알아내어 암호화된 데이터를 복호화한 것이다. 이는 의사난수의 문제점을 그대로 보여주는 한 예이다.

진정난수는 양자역학에 의거하여 발생시킬 수 있다. 최근 제네바 대학의 연구팀은 이 양자진정



(그림 3) 제네바 대학교의 양자진정난수생성 칩 모델

난수생성기술을 칩화하는데 성공하였다. 이 기술이 칩으로 양산되게 된다면, 모바일 디바이스를 포함한 모든 통신기기에 보안성 향상에 새로운 혁명을 일으키게 될 것이다.

일반적으로 PC에서 온라인 금융을 사용할 때 자동으로 깔리게 되는 키보드 보안 프로그램역시 의사난수를 사용한다. 이때 사용하는 OTP도 의사난수이다. 또한 모바일 기기에서 사용하는 e-commerce 역시 의사난수를 사용한다. AP와의 페어링, 블루투스 페어링 역시 의사난수를 사용한다.

이 모든 디바이스들이 양자진정난수생성칩을 활용하게 된다라는 기존의 암호화 기술을 그대로 사용하며 보안성을 높이는 진정한 혁신을 넘어선 혁명에 가까운 일이 된다.

6. 마무리하며

양자암호통신기술을 포함한 양자정보통신기술은 사용자는 느끼지 못하겠지만 세상의 모든 통신 및 보안기술의 패러다임을 바꾸게 될 것이다. 이제는 더 이상 고전 암호 연구자와 양자기반의 암호 연구자가 서로 다툴 때가 아니다. 서로 협력하여 더욱 더 안전한 통신 기술을 연구할 때이다. 최근 들어 퀀텀포럼과 암호포럼의 공동 연구의 움직임은 국내의 보안통신기술을 한걸음 더 발전시킬 수 있는 기회가 될 것이다.

또한 SK텔레콤은 Global Quantum Industrial Partners를 설립 중에 있다. 이는 지금까지 제조업체를 통한 세계 최초의 기술리더십이 아닌, 자체 기술을 통한 Global 기술리더십을 확보하게 되기 때문에 지금까지와는 차원이 다른 리더십이 될 것이다.

기존 암호 연구자들과 양자기반의 암호 연구자들의 움직임과 이를 기반으로 한 SK텔레콤의 Global 리더십의 확보는 단지 SK텔레콤만의 리더십이 아닌 대한민국의 21세기 양자기술 시대의 리더십으로 확장될 것이다.

저 자 약 력

곽 승 환

이메일 : kwaksh@sk.com

- 1997년 홍익대학교 전자공학과
- 1997년 SK텔레콤 입사
- 2005년 세종대학교 정보통신대학원
- 1997년~2011년 CDMA교환기 및 Packet Data 서비스 개발
- 2011년~현재 SK텔레콤 ICT기술원 Quantum Tech. Lab 랩장