금융보안연구원
Financial Security Agency

Best Security Partner Vol. 2011-018

이슈 리포트
ISSUE REPORT

발행처 · 금융보안연구원 발행인 · 곽창규 발행월 · 2011년 10월

차세대 보안기술, 양자암호

목 차

작성 : 이수미 선임연구원

* 문의 : 금융보안연구원 u-금융연구팀 이수미 선임연구원(02-6919-9134, smlee@fsa.or.kr)

1. 서 론

현대 정보보호시스템에서 이용하는 암호기술은 수학적인 문제를 기반으로 설계되어 문제의 크기가 증가함에 따라 그 안전성을 입증하고 있다. 예를 들어 Rivest, Shamir, Adleman 세 사람이 개발한 RSA 공개키 암호체계는 매우 큰 수를 소인수분해하기 매우 어렵다는 점(문제)을 이용한다. 즉 수학적으로 소인수분해 문제는 문제의 크기가 증가함에 따라 계산시간이 지수 함수적으로 증가하게 되며 따라서 송신자와 수신자가 충분히 큰 숫자의 소인수분해 문제를 공개키로 사용한다면 도청자가 암호문을 해독하기는 현실적으로 불가능하게 된다. 그러나 이러한 수학적 계산복잡성에 기초한 암호체계는 슈퍼컴퓨터나 양자 컴퓨터와 같은 초고속 컴퓨팅으로 인해 그 안전성에 의문이 제기되었다. 그 일환으로 1994년 AT&T의 Peter Shor가 양자컴퓨터를 이용한 소인수분해 알고리즘을 개발함으로써 양자컴퓨터가 개발이 되면 RSA 암호체계는 해독이 가능한 것으로 판명되고 있다[1]. 이러한 보안상의 문제로 인해 양자암호(Quantum Cryptography)가 등장하게 되었고 양자암호는 수학적 알고리즘에 기초한 현재의 암호화는 달리 물리학에 기초한 새로운 암호기술이 적용된 기술이다.

양자암호는 빛의 양자 역학적 특성을 이용한 암호화 기술이다. 이러한 양자암호 기술은 보내는 사람이 단위 시간당 한 개의 광자를 보내면서 편광의 방향을 직교 0도 및 90도를 주거나 대각선 45도 및 135도를 주는 2가지 방법 중 한 방법을 택해 그 중 한 방향으로 빛을 편광시켜 보낸다. 결국 송신자는 편광 방향을 0도, 90도, 45도, 135도의 네 가지 중 임의의 한 방향으로 보내는 것을 의미하고 발신자 입장에서도 검광기를 네 가지 방향 중 임의로 조정해 가면서 광자를 검출한다. 이후 대외적으로 자신이 사용한 편광의 방향이 직교인지 대각선인지를 서로 밝혀 이 중 같은 방법을 택한 정보를 암호키로 사용하게 된다. 이러한 양자암호는 도청이 불가능하기 때문에 안전하다고 전문가들은 전하고 있다. 그 이유로 양자암호는 측정에 의해 양자상태가 교란된다는 양자역학의 기본원리를 이용하기 때문이다. 즉 공격자는 암호키를 도청할 수 있으나 전송자와 수신자가 모르게 시도할 수는 없으며 암호키를 완전히 알아내는 것 또한 불가능하다는 것이다. 이것이 양자암호의 가장 중요한 장점이자 핵심이다.

현재 양자암호 기술은 선진국에서 기업들이 상용 양자 키분배 암호제품을 생산하는 단계이며, 특히 미국 경우 국방첨단연구사업국(Defense Advanced Research Projects Agency, DARPA)이 군용으로 무선통신을 위한 양자암호화 기술을 개발했다. 국내에서도 국가소프트과학 연구계획 프로젝트인 '사이버공간기술 국가발전전력 연구'에서 선정된 6대 분야 중 하나로 지정되었으며 양자암호에 대한 관심도가 국내·외적으로 높음을 알

수 있다. 향후 양자암호는 국가 간 기밀 통신 뿐 아니라 전기, 가스, 수도망 등의 중요한 인프라의 통신 보호를 위해 활용될 수 있으므로 미래의 보안 시스템에 가장 핵심적 역할을 할 수 있을 것으로 예상된다. 따라서 전문가들은 국가 정보보안 주권 확립의 차원에서도 양자암호관련 기술의 개발이 필요함을 전하고 있다.

2. 양자암호 이론

양자암호에 대한 설명에 앞서 양자 컴퓨터(Quantum Computation)에 대해 간략히 정리하면 다음과 같다.

양자 컴퓨터는 데이터 처리를 수행하기 위해 중첩(Superposition)과 얽힘(Entanglement) 같은 양자 역학적 현상을 동작 원리로 사용하는 연산 기계 장치로 정의할 수 있다. 이를 이해하기 위해 양자역학에 대해 살펴본다. 양자역학은 파동-입자 이중성을 전제한다. 물질의 아(亞)원자적 단위, 즉 원자 이하의 모든 실체는 우리가 보는 관점에 따라 때로는 파동처럼, 때로는 입자처럼 행동하는 양면성을 갖고 있다. 입자와 파동은 전적으로 성질이 다르지만 아원자적 단위는 파동에서 입자로, 입자에서 파동으로 변형을 계속한다. 이를테면 원자가 때로는 파동으로 행동하기도 하고, 빛이 때로는 입자로 작용하기도 한다. 원자 이하의 실체들이 파동 상태에 있을 때에는 공간적으로 떨어져 있는 수 많은 장소에 동시에 존재한다. 가령 전자는 한 곳에 있지 않고 동시에 모든 곳에 존재할 수 있다. 이 때, 입자가 동시에 여러 개의 상태에 있는 것을 **중첩 현상**이라 한다. 또한 양자 세계에서 두 입자는 아무리 멀리 떨어져 있다 하더라도 서로 연결되어 있다. 따라서 한 입자의 상태가 측정되면 다른 입자의 상태는 즉각적으로 결정된다. 이처럼 두 입자가 거리와 무관하게 결합되어 상태에 영향을 미치는 상호작용을 **얽힘 현상**이라 한다.

양자 컴퓨터는 이와 같은 양자역학의 중첩 현상과 얽힘 현상을 활용한다. 디지털 컴퓨터에서 정보의 기본단위인 비트 상태는 0 이거나 1이다. 그러나 양자비트(큐비트)라 불리는 양자정보의 기본단위는 중첩 현상으로 인해 0과 1 두개의 상태를 동시에 가질 수 있다. 또한 두개의 큐비트는 얽힘 현상으로 인해 4개의 상태(00, 01, 10, 11)를 동시에 공유하며 같은 원리로 3 큐비트가 얽힐 때는 8 개, 4 큐비트는 16 개의 상태를 동시에 갖는다. 양자 컴퓨터는 이러한 여러 개의 상태를 동시에 지닐 수 있고, 모든 상태에 동시에 작용할 수 있기 때문에 디지털 컴퓨터와는 달리 단지 한 개의 처리장치로 수 많은 계산을 병렬 수행할 수 있다.

이러한 양자 컴퓨터 개발이란 연산 처리를 위한 양자 역학적 현상을 제어하는 기계 장치를 만드는 것과 양자 상태를 이용하여 새로운 데이터 처리 알고리즘을 개발하는 것으로 크게 나눌 수 있다[2].

양자계산에 의해 공개키 기반의 시스템에 위협이 있음이 알려진 반면 안전하게 암호키를 분배하거나 데이터를 전달할 수 있는 것 또한 가능한 것이 양자역학이다. 양자상태에서 암호키 분배(혹은 양자 암호)의 안전성은 양자 중첩상태에서의 측정에 기인한다. 즉, 양자암호에서는 양자역학에서 정보를 얻기 위해서 필연적으로 사용해야하는 수단으로의 측정과 측정 시 양자상태가 교란되는 양자역학의 기본원리가 적용된다. 이는 암호문을 만드는데 필요한 암호키를 양자암호 통신으로 공유하고자 할 때 도청자가 존재할 경우, 도청자 역시 정보 추출을 위해 측정을 진행해야하며 이는 양자상태의 교란을 가져오게 되어 결국 데이터에 대한 변형을 감지하는 계기를 제공한다. 역으로 측정은 양자상태의 교란을 가져온다는 양자역학의 기본 원리에 의해 양자상태에 대한 정보를 얻어내면서 전달되는 양자상태를 교란시키지 않는다는 것은 불가능하다. 결국, 현 암호 시스템에서는 데이터를 복제하고 이를 재생하여 공격할 수 있는 위협이 가능하며 이처럼 측정이 양자상태를 교란시켜 변화를 준다하여도 양자상태를 복제할 수 있다면 이 또한 양자암호의 위협이 될 수 있다. 하지만 이러한 방식의 위협 또한 “알져지지 않은 상태를 복사하는 것은 불가능하다”라는 “복사불가능의 정리(No Cloning Theorem)”에 의해 위협의 어려움이 증명되었다[3]. 예를 들어 두 사용자가 1천 큐비트의 양자정보를 교환할 때 5백 큐비트를 서로 확인한다고 가정할 경우 전송과정이 완벽하고 교란이 없었다면 5백 큐비트가 서로 동일한 상태일 것이다. 이론적으로 도청자에 의해 교란이 발생되면 두 사용자가 서로 다른 양자정보를 갖게 될 확률은 1/4이 된다. 즉 5백 큐비트 중 125큐비트 정도가 서로 다른 정보를 갖게 된다. 이는 정보 전달 과정에서 생기는 예상 에러 수보다 훨씬 많은 수에 해당된다. 이런 상태에 도달된다면 두 사용자는 도청된 사실을 감지하여 암호키를 사용하지 않는다.

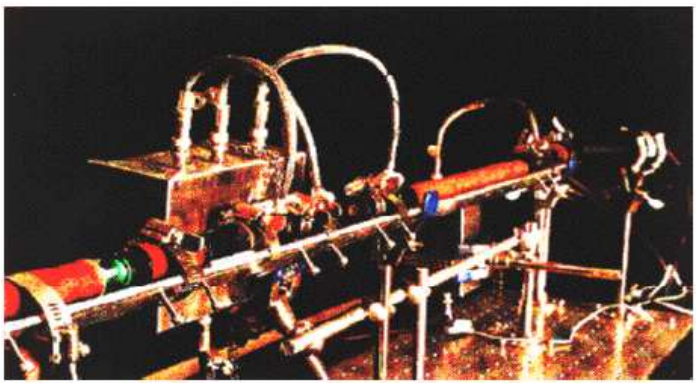

그림 1. 세계 최초의 양자 암호키 전송장비

이러한 양자역학을 이용한 암호키를 분배하는 최초의 양자키 분배기법은 Bennett과 Brassard에 의해 BB84라 명칭되는 기법이 제안되었다[4]. BB84 기법은 도청자가 흔적을 남기지 않고 성공할 확률이 미미함으로 양자암호키 분배는 안전한 암호체계임을 증명하였다. 그림 1은 BB84 기법을

실험하기 위해 Bennett과 Brassard에 의해 제작된 장비이며 이를 이용하여 30cm의 거리에서 양자 암호키를 분배하는 실험에 성공했다. 이후 Ekert, Mermin 등 연구가에 의해 다양한 양자 암호키 분배기법이 설계되었고 양자서명, 양자인증, 다자간 양자통신기법 등 다양한 분야에서 연구가 진행되고 있다.

그림 2. 양자암호통신 방법

다음은 양자 암호키 분배에 대한 설명이다. 고등과학원 김재완 교수는 양자암호를 3D영화에 비유했다. 즉 3D 영화를 볼 때 착용하는 특수 안경(편광안경)의 왼쪽은 수직편광(↕)만, 오른쪽은 수평편광(↔)만 통과시킨다. 따라서 편광안경을 쓰고 영화를 보면 왼쪽 눈과 오른쪽 눈이 보는 화면이 달라서 3차원을 느낄 수 있다. 이를 양자암호에 적용하면 전송자가 수신자에게 비트 0이나 1을 보내기 위해 각각 대각 편광(↗↙)과 역대각 편광(↘↖)을 쓴다고 가정하고 그림 2와 같이 수평/수직편광 방식을 'ㄱ방식', 대각/역대각 방식을 'ㅅ방식'이라고 하자. 양자암호통신에서는 비트 하나를 표현하기 위해 광자 하나, 즉 단일광자를 사용한다. 'ㄱ방식'으로 보낸 단일광자는 'ㄱ방식'으로 측정하면 보낸 대로 비트가 정확하게 전달된다. 하지만 'ㅅ방식'으로 측정하면 비트를 정확하게 전달할 수 없다[5].

그림 3과 같이 전송자 (A)는 'ㄱ' 또는 'ㅅ'방식을 혼합하여 비트를 보내고 수신자 (B)는 두 방식을 혼합하여 측정해야 한다. 이후 수신자와 전송자는 어떤 비트로 측정되었는지 밝히지 않고 각 광자에 대해서 송수신 방식인 'ㄱ'인지 'ㅅ'방식인지만 밝힌다. 즉 각 비트에 대해 송수신자는 수평/수직편광인지 아님 대각/역대각 방식인지에 대해서만 공개한다. 만일 송수신자가 같은 방식으로 보내고 받았다면 송수신자 간에 공유된 비트는 100%로 동일할 것이다. 그림 3과 같이 맞게 온 비트는 '1,1,1,0,0'이므로 송수신자는 서로 '1,1,1,0,0'를 공유하게 된다. 이때 공유되어지는 비트는 일회용 암호 키로 사용될 수 있다.

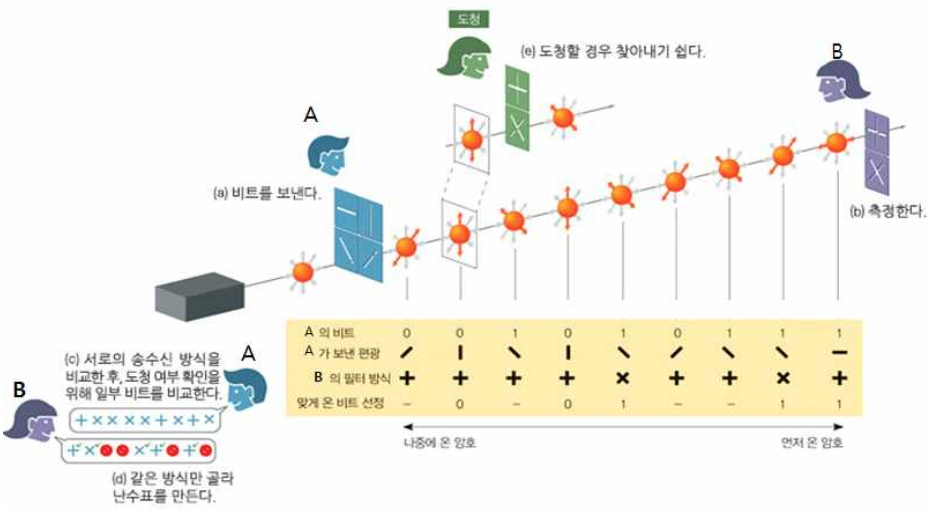

그림 3. 양자 암호키 분배 원리

3. 양자암호의 알려진 결함

양자암호 기술은 지금까지 살펴본 바와 같이 완전한 암호체계를 이룰 수 있는 기술로서 이는 어떤 방식으로든 양자상태를 교란시키지 않고서는 양자계를 측정하기 어렵다는 양자역학에 바탕을 두고 있다. 그러나 현실 세계에서 양자암호 체계는 완전할 수 없음을 몇몇 전문가에 의해 밝혀지고 이를 보완하기 위한 노력들이 끊임없이 이루어지고 있다. 양자암호의 결함은 실제 환경으로부터 오는 일상적인 노이즈로 인해 어느 정도 오류가 발생될 수 있다. 양자물리학자들은 두 사용자 간에 공유될 데이터의 불일치가 20%이하일 때 보안이 유지되는 것으로 간주해 왔다. 그러나 양자물리학자인 Hoi-Kwong Lo의 연구팀은 Switzerland, Geneva주에 위치한 회사인 ID Quantique(IDQ)가 판매 중인 양자암호 체계를 키 간의 불일치 정도가 20%를 넘지 않도록 유지하면서 해킹에 성공하였다고 밝혔다. 현 양자암호 체계에서 전송자는 연속적인 비트들의 편광 방향을 즉시 변경할 수 없다. 이전 비트와 다른 편광 방향을 갖는 비트를 보내려할 때마다 광자에 걸리는 전압을 변경해야만 하기 때문에 공격자가 이 순간 통신망을 급습하여 비트를 가로챌 수 있다고 연구팀은 전하고 있다. 사실 공격자가 측정 후 비트를 그대로 전송한다면 측정으로 인해 오류가 20% 이상이 발생될 수 있으나 공격자가 비트들의 편광 방향을 조금씩 변경시켜 도청으로 인해 발생하는 오류를 19.7%까지 낮출 수 있음을 보여주었다. 이에 양자물리학자들은 상용버전의 양자암호체계는 오류가 겨우 8%만 넘어도 중단되므로 Lo연구팀이 주장한 위협에 대해 안전성을 주장하였으나 이와 같은 결함을 보완하기 위해 노력해야함을 주장했다[6].

4. 양자암호 기술동향

최초의 양자 암호통신은 1984년 IBM의 H. Bennet에 의해 발표된 BB84 이후 기초적인 원리들은 실험을 통해 상당 부분 증명된 바 있으나 구현에 있어서 전송 거리의 확대와 암호키 생성 속도 등을 개선해야 하는 문제점이 남아있다.

2003년부터 미국 DARPA의 지원 하에 BBN 테크놀로지는 하버드대, 보스턴대 연구진과 공동으로 최초의 양자 키 분배 네트워크(Quantum Key Distribution)를 개발하였고 최근 일본 정보통신연구기구(NICT)와 미츠비시전기, 일본 전기 주식회사(NEC), 일본 전신 통신 회사(NTT)는 도쿄 오테마치와 고가네이, 하쿠산, 혼고의 4개 거점에 양자열쇠 분배장치를 설치하고 10km에서 최대 90km에 걸친 전송거리에서 장치가 안전하게 작동하는지 확인하였다. 이로써 양자 암호의 동영상 전송 네트워크는 세계 최초로 성공하였다. 이를 기반으로 NICT는 시험운용을 거쳐 이 기술을 2014년까지 실용화할 것으로 예상하고 있으며 정부기관 외에 발전소, 가스, 수도망 등 주요한 인프라 통신을 보호하는 수단으로 적용한다는 목표를 갖고 있다[7].

그림 4. 양자암호 전송을 이용한 휴대전화 소프트웨어 개발

또한 NICT와 미츠비시전기는 공동으로 양자암호 전송을 이용함으로써 휴대전화 단말기 사이의 통화가 도청이 불가능하도록 하는 것을 물리적으로 보증한 원타임 패드 휴대전화 소프트웨어를 개발했다고 밝혔다. 광회선을 사용한 양자암호 전송으로 양자간 암호키를 배분하고 통화자는 각각의 양자암호 전송장치에서 휴대전화에 암호키를 다운로드하여 암호통신을 수행하는 방식이다. 이를 원타임 패드 휴대전화 소프트웨어로 명칭했으며 개발된 소프트웨어는 음성 데이터와 같은 길이의 암호키로 암호화를 하기 때문에 긴 암호키를 필요로 한다. 가령 양자가 통화내용을 10분간 암호화하기 위해서는 1,200,000바이트의 암호키를 사전 공유해 놓을 필요가 있다. 원타임 패드 휴대전화는 암호키 전송용 PC를 통해 양자키 전송장치와 접속할 때 원타임 패드용 암호키로 공유한다. 또한 사용된 암호키는 일회용으로 하고 암호화 또는 복호처리가 종료된 시점에서 단말기에서 소거된다. 따라서 단말기의 분실이나 도난이 발생하였을 때 단말기에서 추출한 암호키를 이용하여 암호화 통화내용을 복호화하는 도청은 불가능하다고 주장하고 있다. 추가적으로 연

구팀은 앞으로 3~5년 후 이번 원타임 패드 휴대전화의 실용화를 목표로 하고 있다고 밝혔다[8].

영국의 파이낸셜타임스는 브리스틀대학과 일본의 도호쿠 대학, 이스라엘 바이츠만 연구소, 네덜란드 트웬테 대학 연구진으로 구성된 국제 연구팀이 양자컴퓨터에 필수적인 광회로 칩을 개발하였으며 이는 전기가 아닌 빛으로 정보를 처리 저장할 수 있어 이를 기반으로 한 초고속 양자컴퓨터 생산이 가속화될 전망이라고 보도했다. 또한 광회로 칩 개발을 주도한 제레미 오브라이언 영국 브리스틀대학 교수는 양자컴퓨터와 관련된 많은 사람들이 양자컴퓨터가 나오는데 적어도 25년이 걸릴 것으로 내다봤지만 광회로 칩의 기술 발전으로 5년 내에 양자 컴퓨터가 나올 것으로 예상했다. 또한 양자암호 기술은 미국, 유럽, 일본 등 선진국을 중심으로 세계적으로 활발한 연구가 이루어지고 있다. 미국의 경우 CIA, NSA, NASA 등의 국가 안보 관련 기관을 중심으로 유럽의 경우에는 유럽 공동체 차원의 연구 지원이 이루어지고 있다. 양자암호 통신 기술은 기술적인 측면에서 기존의 광통신 기술을 활용하며 통신 사업자들이 기 매설한 광섬유 시설을 곧바로 이용 가능하므로 향후 대규모 상용화가 가능할 것이라는 것이 대체적인 의견이다.

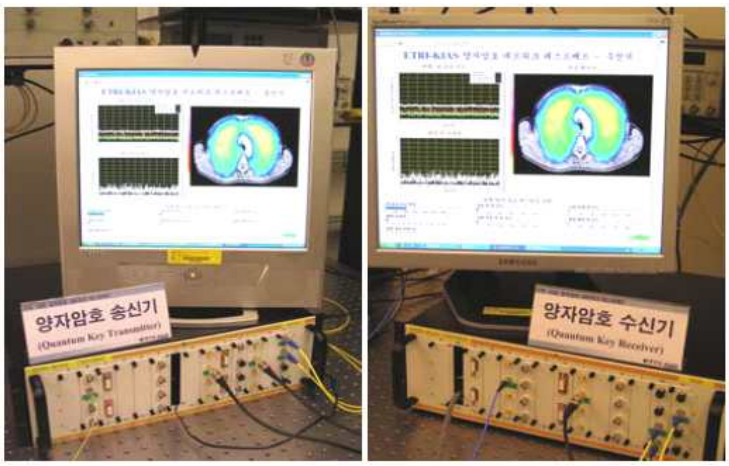

그림 5. 양자암호 송신기와 수신기

양자암호의 중요성은 국내에서도 관심의 대상이 되고 있다. 한국과학기술기획평가원(KISTEP)은 10년 후 국내에서 가장 필요한 10대 미래 유망 기술 중 하나로 양자암호를 선정하였다. 이처럼 양자암호의 중요성은 국내에서도 관심의 대상이 되고 있다. 2005년에는 과학기술부의 창의적연구진흥사업을 통해 데이터를 암호화하는 양자 암호화 방법을 개발하였으며 한국방송통신전파진흥원은 '양자 기반 차세대 통신방식' 등 양자 통신 기술 연구의 기반을 다져나갔다. 국내에서 양자암호 기술에 대한 성과로 연구진은 25km 상용 광섬유를 이용한 실시간 연속동작 양자암호 통신 테스트 베드를 그림 5와 같이 구축하여 양자암호통신의 전 과정을 구현하였고[9], 이후 장거리 양자암호의 핵심기술인 장거리 양자메모리 개발에 주축을 이루었다. 그동안 양자암호는 100km를 벗어날 경우 광통신의 거리제약 등을 이유로 제 기능을 하지 못했기 때문에 장거리 통신 등에 상용화되려면 장거리 양

자암호 기술 확보가 필수라는 게 학계의 설명이며 이 같은 상황에서 최대 10시간까지 양자정보를 저장할 수 있는 새로운 방식의 양자메모리 프로토콜을 개발하여, 지금까지 불가능하다고 여겨왔던 100㎞ 이상의 장거리 양자통신을 가능하게 하는 기초를 마련하는 등 세계 양자정보처리 통신의 핵심기술을 선점하고 선도할 수 있는 계기를 마련하였다[10].

5. 결론

지금까지 새로운 차세대 통신보안기술로 주목받고 있는 양자암호에 대해서 살펴보았다. 현 암호기술은 인터넷의 발달과 더불어 상업적으로 다양하게 응용되고 있다. 예를 들어 전자상거래에서 결제용 비밀번호 등과 같은 중요한 개인의 정보를 암호화하는 암호기술들이 적용되어 안전성을 보장하고 있다. 이처럼 암호기술은 다양한 환경에서 데이터 보호를 위해 적용되고 있지만 고속화되는 컴퓨팅 성능 등의 이유로 보안상의 문제가 발생되고 있다.

양자암호 기술은 현존하는 위협으로부터 안전하게 암호통신을 이룰 수 있는 기술이다. 기반 기술인 양자암호는 통신, 금융 등 주요 인프라 보호를 위해 활용될 수 있으며 향후에는 국가 차원의 기밀정보를 보호할 수 있는 수단으로 자리매김할 것이다. RSA 연구소의 연구책임자인 칼리스키 박사는 양자암호기술을 “암호기술의 주요한 패러다임 변혁”이라고 표현하고 “현 암호기술과 양자암호 기술의 결합은 더욱 안전한 통신체계를 실현하는 강력한 도구”라고 말하고 있다. 이처럼 암호학자들은 양자암호의 중요성에 대해 인지하고 있고 양자암호 통신의 각 분야 기술이 아직은 기초 연구 수준에 있지만 세계적으로 그 중요성이 인식되어 대규모 투자가 이루어지는 분야이므로 기술 발전 추세에 대처할 수 있는 기반 기술을 확보하는 연구가 지속적으로 수행되어야 한다고 전한다.

현 암호기술에 의존도가 높은 분야 중 하나는 바로 금융권일 것이다. 이는 다양한 위협으로부터 금융 서비스를 이용하는 사용자의 자산을 완벽하게 보호하는 것이 가장 중요한 핵심이기 때문이다. 하지만 현존하는 수학적 계산 복잡성에 기초한 암호체계는 슈퍼 컴퓨터나 양자 컴퓨터와 같은 초고속 컴퓨팅으로 인해 암호기술의 안전성에 의문이 생기게 되었다. 따라서 안전한 전자금융서비스를 위해서는 향후 현 암호기술의 대처 방안으로 고려되고 있는 양자암호 기술연구를 지속적으로 수행해 나갈 필요성이 제기되고 있다.

<참고문헌>

[1] P.Shor, In Proc. of the 35th Annu. Symp. on Foundations of Computer Science, IEEE Computer Society Press, Los Alamitos, California, 1994, pp.124
[2] 이인식, 'IQ 2000' 컴퓨터 나온다, 과학문화연구소
[3] W. Wootters and W. Zurek, Nature vol.299, pp. 802~803, 1982
[4] Charles H. Bennett, Gilles Brassard, Quantum Cryptography: Public key distribution and coin tossing, International Conference on Computers, Systems & Signal Processing Bangalore, India, 1984.
[5] 김재완, 창과방패의 대결, 양자컴퓨터와 양자암호, 과학동아, 2011
[6] Feihu Xu, Bing Qi, Hoi-Kwong Lo, Experimental demonstration of phase-remapping attack in a practical quantum key distribution system, Quantum Physics, 2010
[7] 최경모, 도청과 해킹이 불가능한 안전한 양자암호방식, 컴퓨터정보공학과 IT정보메일9호, 2011
[8] http://www2.nict.go.jp/pub/whatsnew/press/h22/100902/100902.html
[9] 한국전자통신연구원 양자정보통신팀 물리학과 첨단기술, 2006
[10] 한국연구재단, 장거리양자통신 양자암호 가능 양자메모리 프로토콜 개발, 2009