문명 발전의 역사를 정보처리와 관련해서 볼 수 있다. 생물체는 처음에 DNA에 정보를 축적하기 시작했고, 신경세포의 발달로 뇌에 정보를 축적하기 시작했다. 물질들이 물리적으로 화학적으로 상호작용하는 것처럼, 생물체는 이러한 상호작용 방식을 발전시킨 감각기관으로 주변을 탐색하고 서로 정보를 교환하고, 뇌를 비롯한 중추신경계는 정보를 저장하고 정보를 처리하는 기관으로 발전했다. 정보교환의 수단은 사람의 경우 언어로 발전했고, 역사 시대는 이 언어를 글과 책으로 남긴 역사의 저술과 함께 시작되었다. 계산은 정보처리의 한 유형으로 볼 수 있는데, 동양에서 발명된 주산은 최근까지 쓰였고, 고대 그리스의 기계식 계산기 앤티키테라는 오랜 세월 동안 잊혀졌다가 20세기 후반에야 발견되고 복원되었다.

도 영국의 찰스 배비지는 영국 왕실의 후원으로 본격적인 기계식 계산기를 설계하였다. 그렇지만 배비지 기계가 제대로 만들어진 것은 20세기 후반에 와서의 일이다.

19세기에 맥스웰은 전기와 자기현상을 통합하여 빛을 포함한 전자기파동을 발견하였고, 20세기를 맞으면서 플랑크와 아인슈타인에 의해 시작된 빛에 대한 양자역학적 이해는 1960년대에 글라우버 등에 의해 양자광학으로 꽃피었다. 이 업적으로 글라우버는 작년인 2005년에 노벨물리학상을 수상하였다. 전자기 현상은 이전에 기계적인 방식에 의존하던 정보전달은 물론 저장, 처리 등의 중요한 수단으로 이용되게 되었고, 20세기 후반 정보혁명을 주도하였다. 여기에는 양자물리학을 바탕으로 한 반도체와 레이저 등에 의한 전자컴퓨터와 광통신이 큰 역할을 하였다.

첨단 광학 및 광기술 해설

양자정보과학과 양자광학

김재완*

수 천 년 동안 지속된 역사시대는 17세기 이후 근대과학기술 혁명을 거치면서 갈릴레오와 뉴턴의 고전역학체계를 낳았다. 고전역학의 발전과 함께 기계기술이 발전하면서, 시카드, 파스칼, 라이프니쯔 등 수많은 수학 및 과학 기술자들이 기계식 계산기를 발명하였는데, 그 중에서

IBM의 란다우어는 물리학의 발달에 따른 정보혁명을 '정보는 물리적인 것이다 (Information is physical.)' 이란 말로 요약하였다. 존 휠러 교수는 자신의 학문적 여정을 세 단계로 나눠, 어렸을 적에는 모든 것이 입자(particle, 고전역학적 세계관)라고 생각했는데, 다음에는

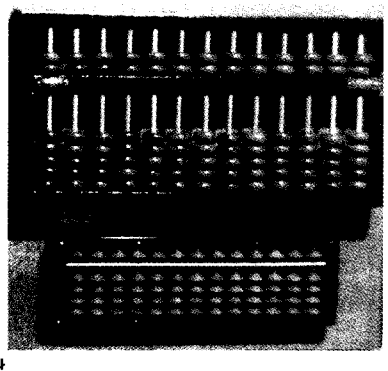

그림 1. 주판

그림 2. 앤티키테라 : 고대 그리스의 기계식 계산기(보스턴 과학박물관에서 저자 촬영), 발견된 파편과 엑스레이로 촬영된 파편의 내부와 복원된 앤티키테라.

* 고등과학원, jaewan@kias.re.kr

그림 3. 찰스 배비지와 배비지 기계

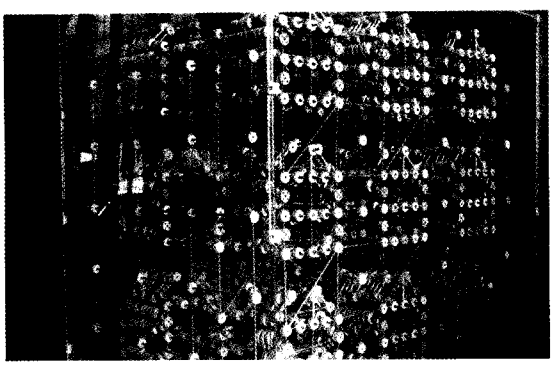

그림 4. 조립식 장난감(Tinker Toy)으로 구성한 디지털 컴퓨터 : 보스턴 과학박물관 입구에 진열되어 있다 (저자 촬영).

그림 5. 휠윈드 : 제2차 세계대전 중 항공시뮬레이션을 위해 사용된 고속 컴퓨터

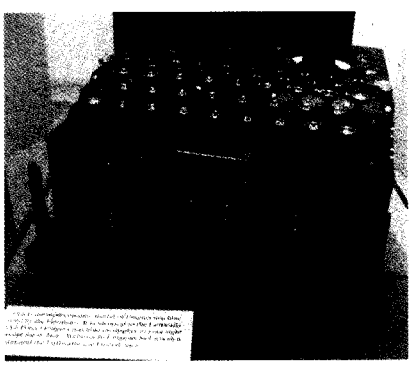

그림 6. 에니그마 기계 : 제2차 세계대전 중 독일군이 사용한 암호기계

장(場 = field, 양자물리학적 세계관)이라고 생각하게 되었고, 이제는 모든 것이 정보(information)이라고 생각하게 되었다고 하였다. 그는 이것을 'It from Bit.' 라는 말로 요약하였는데, 모든 것이 정보라는 것이다. 이러한 세계관은 사실 동양에서 수천 년 전부터 지혜로 삼아 온 음양이론을 바탕으로 한 주역에서도 엿볼 수 있다.

여기서 정보(情報)라는 우리 용어에 대해 잠깐 주목해 보자. 같은 한자를 쓰는 문화권이지만, 한국과 일본은 information만 정보(情報)라고 하는 것이 아니라, 첩보활동에 관련된 intelligence도 같은 정보(情報)라는 단어를 사용하고 있다. 중국과 대만도 intelligence는 같이 정보(情報)라고 하지만, information은 각기 신식(信息)과 자신(資訊)이라고 쓰고 있다. 중국과 대만에서는 우리의 국가정보원과 정보통신부를 비슷한 기구로 오해할지도 모르겠다.

정보처리 분야는 제2차 세계대전 중 적국의 암호통신을 해독하기 위해 컴퓨터의 발명이 이루어지면서 발전했다. 영국은 콜로수스라는 컴퓨터를 만들어 독일의 암호기계 에니그마로 만들어진 암호문을 해독하였다. 영국 정보부를 위해 일하던 튜링은 현대 컴퓨터의 정형인 튜링기계를 비롯한 현대 계산과학이론의 토대를 마련하였다. 처치와 튜링의 정리에 의하면 무한히 긴 정보 저장 테이프가 있으면 몇 가지 논리연산을 할 수 있는 모든 계산기계는 계산속도에 있어서 차이는 있을지라도 본질적으로 동등하다. 보스턴 과학박물관 입구에는 MIT 학생들이 팅커토이라는 장난감으로 만든 삼목게임(Tic-Tac-Toe)용 컴퓨터가 진열되어 있다. 이것은 물론 무한히 긴 정보저장테이프는 없지만 계산기계의 동등성을 보여주는 좋은 예가 될 수 있겠다. 에니액이나 휠윈드 같은 최초의 고속 컴퓨터는 요즘의 노트북 컴퓨터보다 몇 십만배나 컸지만, 그 능력은 훨씬 떨어지는 것이었다.

제2차 세계대전 중 진행된 암호전쟁은 현대에 시작된 것이 아니다. 고대에도 막대에 감은 천이나 종이에 메시지를 적어서 푼 후 전달하는 시털리을 비롯해 갖가지 암호 방식이 사용되었다. 암호를 만들고(cryptology) 이를 공격하는(cryptanalysis) 암호전쟁은 20세기 후반의 정보혁명에 뒤이어 그 극에 달하고 있다.

한편 통신 분야에서는 벨연구소의 새넌에 의해 정보량

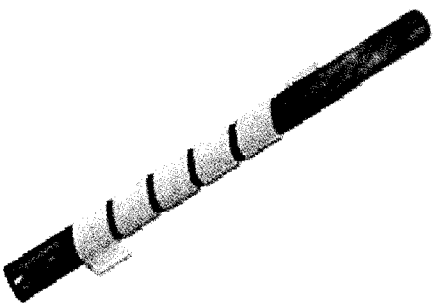

그림 7. 시텔리(Scytale) : 막대에 감은 천이나 종이에 메시지를 쓴 후, 풀어서 메시지를 보낸다.

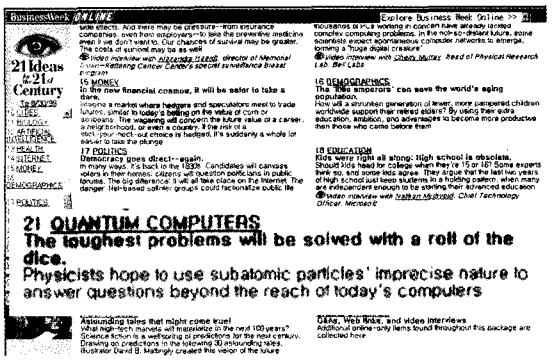

그림 8. 양자컴퓨터를 21세기 주요 화두로 선정한 비즈니스위크 기사 : "가장 어려운 문제를 주사위를 굴리는 방법으로 풀게 될 것이다"는 표현이 나온다.

을 정보 엔트로피로 측정하는 정보 압축과 통신채널 용량에 대한 정량적인 연구가 이루어지게 되었다. 새넌의 연구는 정보의 저장 및 전송을 비롯해 정보처리연구 전반에 걸쳐 아주 위대한 업적으로 여겨진다.

앞에서 언급한 바와 같이 양자물리학을 바탕으로 한 반도체와 레이저 기술은 0과 1, 즉 비트(bit)를 사용하는 튜링과 새넌의 정보과학을 한층 효율적인 기술로 승화시켰다. 그러나 여전히 양자물리학의 적용이 하드웨어에 국한되어 있던 상황에서 이제 양자물리학이 정보 그 자체에까지 적용되는 진정한 의미의 양자정보과학이 등장하게 되었다.

반도체 소자의 집적도가 18개월에 2배로 된다는 무어의 법칙으로 대표되는 반도체소자기술의 발달은 2020년경에는 그 한계에 도달하리라는 예측이 지배적인 상황이다. 점점 작아지는 소자에서 나타나는 양자터널링과 같은 양자물리학적인 현상은 기존의 고전 정보기술에는 0과 1을 불분명하게 만드는 '피하고 싶은' 치명적인 현상으로서, 그 연장선상에 서 있는 나노테크놀로지에서는 어떻게 하면 이것을 피할 수 있나 하는 소극적 입장을 취하고 있다. 그 반면에 양자정보과학은 오히려 0과 1이 동시에 될 수 있는 양자역학적인 중첩(superposition)을 비롯하여 기존의 고전정보에서 피하고 싶은 여러 가지 양자물리학적인 현상을 적극적으로 이용하겠다는 입장이다. 1980년대 이후 활발한 연구가 진행되고 있는 단전자(single electron) 소자 연구는 이제 단일광자(single photon)를 다룰 수 있는 양자광학과 함께 양자정보시대를 열어 가고 있다. 그런 의미에서 양자정보과학은 나노과학의 꽃이라고 할 수 있다.

1999년 비즈니스위크 잡지는 21세기를 맞이하면서 21세기의 주요 화두 21 가지를 꼽았는데, 그 중 하나로 양자컴퓨터를 꼽았다. "가장 어려운 문제가 주사위를 던지는 식으로 해결될 것이라"는 표현이 나온다. 아인슈타인은 광전효과이론으로 양자물리학의 토대를 세우고 그 공로로 1921년 노벨물리학상을 받았지만, 양자물리학의 측정과 관련하여 그 확률론적인 면을 도저히 받아들일 수 없었다. 아인슈타인은 양자물리학의 확률론적인 면에 대한 불만을 "신은 주사위 놀음을 하지 않는다"는 식으로 표현하였는데, 비즈니스위크의 기사는 바로 이것을 빗대어서 양자컴퓨터를 표현한 것이다.

양자정보의 기본 개념

큐비트 (Qubit = Quantum Bit)

디지털 정보인 비트(bit=binary digit)는 '0 또는 1'로 나타내는 데에 비해, 보통 양자정보의 단위인 큐비트(qubit=quantum bit)는 서로 완전히 구별되는 두 양자상태 $|0\rangle$과 $|1\rangle$의 선형중첩(linear superposition)으로 나타낸다.

$$|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

여기서 두 기본양자상태 $|0\rangle$과 $|1\rangle$은 원자핵의 스핀방향, 전자의 스핀방향, 원자의 안정된 두 에너지 상태, 광자의 서로 수직된 편광방향 등과 같이 서로 완전히 구별되는 — 내적(inner product)이 0이 되는 — 양자상태이면 된다. $|0\rangle$과 $|1\rangle$은 규격화 (normalization) 조건을 만족하고, α와 β도 $|\Psi\rangle$의 양자확률의 합이 1이 되도록

규격화 조건을 만족하는 복소수다. 즉, $|\Psi\rangle$를 $|0\rangle$ 또는 $|1\rangle$이 되도록 하는 측정을 하면 $|\alpha|^2$과 $|\beta|^2$은 각각 $|0\rangle$ 또는 $|1\rangle$이 될 확률이다.

$$|\alpha|^2+|\beta|^2 = 1$$

$|0'\rangle$과 $|1'\rangle$을 다음과 같이 정의하면

$$|0'\rangle = 1\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

$$|1'\rangle = 1\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

이들을 새로운 기본양자상태로 사용하여 큐비트를 나타낼 수 있다.

$$|\Psi\rangle = \frac{\alpha+\beta}{\sqrt{2}}|0'\rangle + \frac{\alpha-\beta}{\sqrt{2}}|1'\rangle$$

α와 β가 복소수이므로 큐비트는 마치 무한한 정보를 갖고 있는 것처럼 보이지만, 양자정보는 측정이 될 때에 가용(可用)정보가 실현되므로 실제로는 무한한 정보를 갖고 있다고 볼 수 없다.

n비트의 정보는 00...0부터 11...1까지 2^n개의 조합이 가능하지만, n개 중에 하나만 나타낼 수 있는 데에 비해, n개의 큐비트는 $|00...0\rangle \equiv |0\rangle|0\rangle...|0\rangle$부터 $|11...1\rangle$까지 2^n개의 기본양자상태들의 중첩을 한꺼번에 나타낼 수 있다. 양자컴퓨터와 양자계산의 지수함수적인 병렬성은 바로 여기에 있고, 이를 양자병렬성(quantum parallelism)이라고 부른다.

그러나, 양자계산이 진행 중인 동안에는 양자컴퓨터의 레지스터에 양자병렬적인 데이터가 들어있지만, 계산결과를 얻기 위해 양자측정을 하면 이 양자병렬성이 깨어져 비트에 해당하는 정보만 얻을 수 있다. 따라서 양자계산의 과정은 이러한 양자병렬성과 양자측정을 교묘하게 활용해야만 고전컴퓨터에 비해 뛰어난 효율성을 얻을 수 있다. L자릿수의 자연수에 대한 소인수분해의 고전알고리듬이 L에 대해 거의 지수함수적인 계산시간이 걸리는 데에 비해, Peter Shor의 소인수분해 양자알고리듬이 L의 3승 정도의 시간만 걸리는 까닭은 바로 이 양자병렬성에 있다.

양자 얽힘 (Quantum Entanglement)

두 개의 큐비트는 4 개의 기본양자상태 {$|00\rangle \equiv |0\rangle|0\rangle, |01\rangle, |10\rangle, |11\rangle$}의 중첩으로 나타낼 수 있다. 이들 기본양자상태들은 두 큐비트의 기본상태들의 곱으로 나타낼 수 있지만, 이들이 중첩된 두 큐비트의 일반적인 상태는 극히 예외적인 경우를 제외하고는 두 큐비트의 곱으로 나타낼 수 없다. 두 큐비트의 곱으로 나타낼 수 있는 극히 예외적인 경우를 분리가능한(separable) 상태라고 하고, 그렇지 않은 경우를 얽힌(entangled) 상태라고 한다. 분리가능한 상태는, 한 큐비트를 측정하여 어떤 결과를 얻더라도 다른 큐비트에는 아무런 영향도 미치지 않는다. 하지만 얽힌 상태에서는 한 큐비트를 측정하면 다른 큐비트의 상태에 영향을 미치게 된다. 예를 들어,

$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle|1\rangle + |1\rangle|0\rangle)$$

는 얽힌 상태로서, 첫번째 큐비트를 측정하면 $|0\rangle$ 또는 $|1\rangle$로 될 확률이 각각 50 %인데, 그 각각의 경우 두 번째 큐비트는 100 %의 확률로 $|1\rangle$과 $|0\rangle$으로 된다. 멀리 떨어져 있는 두 큐비트가 얽혀 있을 때, 한 큐비트의 측정이 다른 큐비트에 영향을 미치므로 양자역학의 비국소성(nonlocality)을 보여준다. 아인슈타인 등은 이 비국소성이, 어떠한 것도 빛보다 빠른 속도로 전달될 수 없다는 특수상대성이론과 모순된다고 생각했지만, Aspect 등에 의한 양자광학적 실험은 양자역학의 예측이 옳음을 보여주고 있다. 그리고, 첫 번째 큐비트의 측정결과는 양자역학에 의해 확률적으로 결정되기 때문에, 의도적으로 확정된 정보를 두번째 큐비트에 전달할 수는 없으므로, 특수상대성이론의 인과론(causality)과도 모순이 되지 않는다.

양자원격전송 (Quantum Teleportation)

보통 고전적인 이동 또는 전송은 공간을 연속적으로 통과하는 것을 뜻하고, 연속방정식(continuity equation)으로 기술된다. 양자원격이동 또는 전송은 연속방정식으로 기술되지 않는 양자상태 또는 양자정보의 공간이동을 뜻한다. 갑돌이가 을순이에게 그 상태를 전혀 모르는 하나의 큐비트 Q를 양자원격전송으로 보낼 수 있다. 우선 갑돌이와 을순이가 서로 얽힌 큐비트 A와 B를 각각 하나씩 나눠 가진다. 갑돌이는 Q를 A와 얽히게 해서 Bell의 측정을 하여 두 비트의 측정결과를 얻는다 [두 개의 큐비트

는 2×2 즉 네 개의 기본 상태가 가능하고, 넷 중의 하나는 두 비트의 고전정보에 해당한다]. 갑돌이의 측정은, 을순이가 가진 B의 상태를 결정한다. 이제 Q는 측정과 동시에 원래의 상태를 잃어버리고, Q가 갖고 있던 상태의 정보는 B로 옮아가지만 제대로 정리되지 않은 상태에 있다. 갑돌이는 측정결과 얻은 두 비트의 고전정보를 을순이에게 고전적인 통신채널을 통해 알려준다. 을순이는 이 정보를 이용하여 B에 적절한 조작을 함으로써 원래의 Q의 상태를 얻게 된다.

여기서 주목할 것은, 원래 Q의 양자상태를 나타내기 위해서는 두 개의 실수(real number)가 필요하지만, 갑돌이는 이 두 실수를 전혀 모르는 상태에서 두 비트의 고전정보만 전송함으로써 Q의 양자상태를 전송할 수 있다는 것이다. 또, 갑돌이의 측정과 동시에 을순이가 가진 B의 상태가 변하기는 하지만, 양자원격전송이 완결되기 위해서는 두 비트 정보의 고전적인 통신이 있어야 하므로, 빛보다 빠른 이동이 이루어지는 것은 아니라는 점이다. 그리고, Q의 상태는 갑돌이의 측정과 함께 깨어지므로 원본을 복사하는 것과는 다르다. 뒤에 언급되지만, 모르는 양자정보 또는 양자상태는 복사가 불가능하다.

양자압축코드 (Quantum Dense Coding)

한 개의 큐비트를 보냄으로써 고전정보 두 비트를 보낼 수 있다. 우선 갑돌이와 을순이는 서로 얽힌 두 큐비트 A와 B를 나눠 가진다. 갑돌이는 A에 서로 배타적인 네 가지의 조작 중 하나를 가한 후 을순이에게 보낸다. 을순이는 A와 B에 적절한 조작과 측정을 하여 갑돌이가 네 가지 조작 중 어느 것을 하였는지, 두 비트의 정보를 알아낼 수 있다. 양자압축코드와 양자원격전송은, 갑돌이와 을순이가 얽힌 두 큐비트를 나눠가진 경우 한 큐비트의 양자정보와 두 비트의 고전정보가 등가적인 것을 보여준다.

양자정보의 복사불가능성(No-Cloning Theorem)

고전적인 디지털정보는 무한정 복사가 가능한다. 이에 반해, 양자정보는 복사가 불가능하다. 그 간단한 증명은 다음과 같다.

서로 독립인 양자정보 $|\alpha\rangle$와 $|\beta\rangle$를 다음과 같이 재료로 준비된 큐비트 $|0\rangle$에 복사하는 방법을 유니터리 변환 U가 있다고 하자.

$$U|\alpha\rangle|0\rangle = |\alpha\rangle|\alpha\rangle$$
$$U|\beta\rangle|0\rangle = |\beta\rangle|\beta\rangle$$

이제 임의의 상태 $|\gamma\rangle = a|\alpha\rangle + b|\beta\rangle$을 복사하고자 하면,

$$\begin{aligned} U|\gamma\rangle|0\rangle &= U(a|\alpha\rangle + b|\beta\rangle)|0\rangle \\ &= U(a|\alpha\rangle)|0\rangle + U(b|\beta\rangle)|0\rangle \\ &= a|\alpha\rangle|\alpha\rangle + b|\beta\rangle\beta\rangle \\ &\neq |\gamma\rangle|\gamma\rangle = (a|\alpha\rangle + b|\beta\rangle)(a|\alpha\rangle + b|\beta\rangle) \end{aligned}$$

처럼 되어, $|\gamma\rangle$는 복사되지 않는다.

물론 그 상태를 완전히 알고 있는 양자상태는 얼마든지 똑같은 것을 만들 수 있다. 그러나, 그 상태를 모르는 양자정보를 똑같이 복사할 수 있다고 하면 불확정성원리가 성립되지 않을 것이다. 똑같은 양자상태를 무한히 많이 복사해 놓고, 그것들에 무한히 많이 다른 측정을 함으로써 불확정성원리가 허용하는 것보다 더 정확한 상태측정이 가능할 것이다.

만약 양자정보의 복사가 가능하다면 빛보다 빠른 통신도 가능할 것이다. 큐비트를 $S=\{|0\rangle, |1\rangle\}$방식으로 나타낼 수도 있고, $S'=\{|0'\rangle, |1'\rangle\}$방식으로 나타낼 수도 있다. 서로 얽힌 큐비트 $|\Psi\rangle$를 갑돌이와 을순이가 나눠가진 후,

$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle_{갑}|1\rangle_{을} - |1\rangle_{갑}|0\rangle_{을})$$
$$= \frac{1}{\sqrt{2}}(|0'\rangle_{갑}|1'\rangle_{을} - |1'\rangle_{갑}|0'\rangle_{을})$$

갑돌이가 S 방식으로 측정을 하면 을순이가 가진 큐비트는 그와 동시에 $|0\rangle$ 또는 $|1\rangle$이 될 것이고, 을순이가 자신이 가진 큐비트를 여럿 복사해서 여러 가지로 측정을 해보면 갑이 S 또는 S' 중에서 어떤 방식의 측정을 했는지 알아낼 수 있게 된다. 따라서, 빛보다 빠른 통신이 가능하게 된다.

양자측정의 비가역성 (Irreversability of Quantum Measurement)

기본양자상태들의 중첩으로 표현되는 양자상태는 측정 직후 기본양자상태들 중의 하나로 전환되어 원래의 상태

를 잃어 버린다. 즉, 양자상태는 측정으로 인해 다른 상태로 변하고 원래의 상태로 돌아갈 수 없게 된다. 물론 원래의 양자상태가 측정의 기본양자상태 중의 하나였을 경우에는, 원래의 상태나 측정 후의 상태가 같으므로 가역적이지만, 거의 대부분의 경우 양자측정은 양자정보에 돌이킬 수 없는 변화를 일으킨다.

양자정보의 불복사성과 양자측정의 비가역성은 동전의 안팎과 같다. 즉 양자정보를 똑같이 복사할 수 있으면, 원래의 상태를 복사해놓고 측정함으로써 측정의 비가역성을 피할 수 있다. 또 양자측정이 가역적이라면, 양자정보의 측정과 원상태회복을 반복함으로써 양자정보를 정확히 파악해서 똑같은 양자상태를 만들 수 있을 것이다.

이제 양자정보과학의 기본 사항을 바탕으로 양자광학적 양자정보처리에 대해 알아보자.

선형광학적 양자컴퓨터

기존의 디지털컴퓨터가 거의 실리콘 반도체를 바탕으로 이루어진 데에 비하여, 양자컴퓨터는 아직도 어떤 것이 하드웨어가 될지 알 수 없는 상태에 있다. 양자비트 또는 큐비트는 분명하게 구현될 수 있는 서로 직교하는 양자상태를 구현할 수 있어야 하고, 큐비트의 수를 쉽게 확장할 수 있어야 한다. IBM의 디빈첸쪼는 양자컴퓨터의 하드웨어가 만족해야 할 다섯 가지 조건을 내세웠는데, 바로 그 첫째가 이 확장가능한 큐비트이다. 두 번째 조건은 초기 양자상태를 원하는 대로 준비할 수 있어야 한다는 것이다. 컴퓨터 프로그래머들 사이에는 GIGO (Garbage In, Garbage Out)이라는 격언이 있는데, 바로 이 경우에 해당한다. 세 번째로, 큐비트를 원하는 대로 조작할 수 있는 만능게이트(universal gates)를 구비해야 한다. 큐비트 시스템에 원하는 유니터리 조작을 할 수 있는 만능게이트는 단일 큐비트 게이트와 두 큐비트 게이트만 있으면 된다는 증명이 있다. 아무리 큰 유니터리 행렬이라도 행과 열의 두 요소를 제어하는 기본 행렬들의 곱으로 나타낼 수 있는데, 두 요소를 제어하는 기본 행렬의 각 요소는 한 큐비트의 두 기저상태이거나, 두 큐비트의 기저상태이므로, 단일 큐비트 게이트와 두 큐비트 게이트로 충분히 모든 것을 할 수 있다는 것이다. 네 번째 조건은, 기존 디지털컴퓨터의 잡음에 해당하는 것인데,

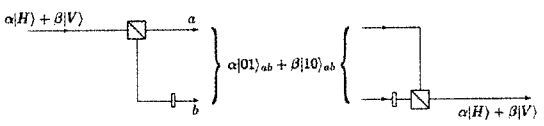

그림 9. 단일광자 큐비트의 편광상태와 공간모드 사이의 변환 방법 : 편광빛살가르개(polarizing beam splitter)와 위상변조(phase shifter)로 쉽게 상호 변환할 수 있다.

계산과정에서 큐비트들이 외부와 상호작용을 통하여 외부와의 얽힘 상태를 만들어서는 안 된다는 것이다. 외부와의 상호작용은 큐비트로 보면 결잃음(decoherence)이 생기는 것인데, 이것은 큐비트가 양자적인 선형중첩상태를 잃어버려 양자병렬성과 같은 양자컴퓨터로서의 특성을 잃어버리게 되는 것이다. 이 결잃음 현상은 양자측정과도 관련이 있으며, 양자역학적인 현상이 고전역학적인 현상으로 되는 것을 설명하는 중요한 메커니즘이기도 하다. 그리고 다섯째로, 양자컴퓨터의 계산 마지막 과정에서 원하는 대로 큐비트의 상태 측정을 할 수 있어야 한다.

현재 양자컴퓨터의 하드웨어 후보로 연구되고 있는 시스템은 핵스핀, 이온덫, 양자점, 초전도체 등 수십 가지에 이르지만, 여기서는 선형광학적 시스템만 살펴보자. 현재까지 가장 많은 큐비트로 만들어진 경우는 핵스핀 양자컴퓨터이다.

단일광자를 큐비트로 사용하면, 우선 광자의 편광상태 또는 공간모드를 큐비트의 기저로 쉽사리 사용할 수 있고, 결잃음이 상온에서조차 아주 작고, 단일 큐비트 조작이 쉬우므로 여러 잇점이 있다. 그러나 광자는 광자와 상호작용을 하지 않으므로 두 큐비트 게이트를 만드는 것이 지극히 어렵다.

두 큐비트 게이트를 만들기 위해, 즉 두 광자가 상호작용하도록 하기 위해 비선형 매체(Kerr)를 쓸 수도 있겠지만, 비선형효과는 빛의 세기에 따라 커지므로 세기가 약한 단일광자로 원하는 만큼의 비선형효과를 얻는 것은 아주 어려운 일이다. 비선형효과를 얻기 위해 매체의 길이를 길게 하다가는 오히려 단일광자 즉 큐비트를 잃어버릴 수도 있다. 또 다른 방법으로 광자와 상호작용할 원자(세슘 등)를 품은 공동(cavity)을 이용하는 방법이 있는데, 광자와 원자와 공동을 다루는 것과 이것으로 큐비트 수를 확장하는 것이나 충분한 크기의 상호작용을 얻기도 쉽지 않다.

이해웅과 김재완은 2000년 단일광자 모드 얽힘으로 단일 광자상태를 양자원격전송하는 방법을 PRA에 발표하였는데, 양자원격전송을 하기 위해서는 벨 측정 중에 두 큐비트 게이트가 반드시 있어야 하므로, 여기서 두 큐비트 게이트를 구현할 수 있는 힌트를 얻을 수 있다. 그 다음해인 2001년 널, 라플람, 밀번 등은 Nature에 KLM 방식이라 알려지게 된 선형광학적 양자컴퓨터에 관한 논문을 발표하였다.

이해웅과 김재완의 양자원격전송에서 벨측정은 선형광학에서 50% 밖에 실현할 수 없다. KLM은 두 큐비트 게이트를 실현하기 위해, 보조큐비트에 조작을 한 후 양자원격전송을 통해 본 큐비트에 옮기는 방법을 고안하였다. 이 방법은 비선형광학을 쓰지 않고, 오로지 선형광학과 측정만으로 확률적인 두 큐비트게이트를 실현하는 것이다. 이 방법은 확률적이긴 하지만 다항식 정도의 부담으로, 즉 지수함수적으로 많은 시행착오를 거치지 않고도, 두 큐비트 게이트를 구현하는 확률을 높일 수 있다. 선형광학적 양자컴퓨터에서 광자 사이의 상호작용은 바로 양자측정의 비선형성에서 나온다고 볼 수 있다. 따라서 그 전의 방식이 결정론적인 데에 비해, 이 방식은 확률적이게 되는 것이다.

라우센도르프와 브리겔은, 2001년부터 2003년에 걸쳐 전혀 새로운 방식의 양자컴퓨터 방식을 개발하였다. 앞에서 언급한 방식은, 큐비트들을 어떤 상태로 준비한 후, 단일 큐비트 게이트와 두 큐비트 게이트를 가해 원하는 다른 상태로 변화시켜가는 네트워크 방식으로서, 말하자면 새로운 양자상태를 빚어내는 (molding; 필자의 표현) 방식인 데에 비해, 이 새로운 방식은 큐비트들이 전체적으로 얽혀있는 클러스터(cluster) 상태로 우선 만든 후, 큐비트들을 하나씩 측정해 나가는 일방향(one-way) 방식이다 (cluster state quantum computing 또는 one-way quantum computing). 필자는 이를 조각하는 (sculpturing) 방식이라고 부른다. 닐슨 등의 연구에 의하면, 클러스터 방식은 원래의 KLM에 비해 훨씬 적은 부담으로 선형광학적 양자컴퓨터를 구현할 수 있다.

선형광학적 양자컴퓨터을 구현하기 위해서는 빛살가르개와 위상변조기 같은 선형광학장치 이외에 즉각적인 (on-demand) 단일광자원과 효율이 높은 광자검출기가 필요하고, 이 방면의 실험연구가 치열하다.

양자컴퓨터는 큐비트 수에 따라 지수함수적으로 늘어

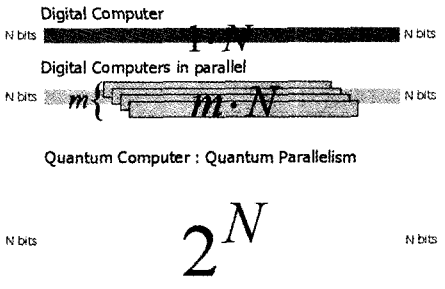

그림 10. 양자병렬성(Quantum Parallelism) : 양자컴퓨터는 계산 중에 계산공간이 기하급수적으로 늘어난다.

나는 힐버트 공간으로 인해 고전 또는 디지털컴퓨터로는 할 수 없는 계산을 할 수 있는 여지가 생긴다. 여기서도 주의해야할 점은, 고테스만-닐의 정리에 의하면 아주 정형화된 상태에 몇몇 정해진 게이트만으로 하는 양자계산은 디지털컴퓨터로도 충분히 효율적으로 할 수 있는 계산이라는 것이다. 디지털컴퓨터보다 훨씬 뛰어난 것으로 현재까지 알려진 양자알고리듬에는, 디지털에 비해 초다항식적으로 빠른 피터 쇼어의 소인수분해, 제곱 정도로 빠른 그로버의 양자데이터검색과 파인먼에 의해 제안된 양자다체문제 등이 있다. 양자데이터검색은 생명정보 분야에, 양자다체문제 시뮬레이션은 나노테크놀로지에 크게 유용할 것으로 기대되고 있다.

양자컴퓨터 이전에도 아주 능력이 뛰어난 것으로 기대되는 아날로그 컴퓨터 방식이 디지털컴퓨터와 경쟁관계에 있었는데, 오류수정이 어렵다는 치명적인 문제가 있었다. 컴퓨터의 연산은 비선형적이고, 비선형성에 의해 나타나는 혼돈(Chaos)적 상황은 조그만 오류가 순식간에 전체 계산을 망쳐놓게 되는 것이다. 양자컴퓨터의 큐비트에도 각 기저의 계수가 복소수로 주어지므로 오류 수정이 어렵지 않을까 염려되었는데, 1996년에 쇼어 등에 의해 양자컴퓨터의 오류 수정 알고리듬이 만들어졌다.

양자컴퓨터는 디지털컴퓨터에 비해 소인수분해를 거의 지수함수적으로 빨리 할 수 있다고 했는데, 이것은 자릿수가 많아질수록 소인수분해 시간이 거의 지수함수적으로 늘어나는 데에 착안하여 만들어진 RSA 암호 방식에 치명적이다.

양자컴퓨터가 디지털컴퓨터에 비해 뛰어난 능력을 발휘하는 것은 양자중첩의 양자병렬성에 기인하는 것인데, 이것으로 디지털통신 보안은 위협을 받게 된 것이다. 이제

〈암호화된 비밀번호〉

갑돌이: 100만원을 갑순이에게 송금.
은행: 비밀번호를 입력해주세요.
갑돌이: ****
그러자 통신라인을 타고 8329라는 숫자가 은행으로 전달된다.
은행: 확인되었습니다.

이 통신을 엿본 도청자가 비밀번호에 8329를 입력하여 갑돌이의 돈을 훔칠 수 있을까.

사실은 갑돌이가 은행과 암호통신을 시작하는 순간 갑돌이와 은행 사이에 비밀키(secret key) 1547이 만들어진다. 보안시스템은 오로지 갑돌이의 컴퓨터와 은행컴퓨터에만 이 비밀키가 알려지도록 작동한다. 갑돌이가 6782를 입력하면, 비밀키가 더해진 8329가 인터넷을 통해 전달되고, 은행컴퓨터는 비밀키를 빼서 6782라는 진짜 비밀번호를 확인한다.

양자물리학의 비가역적인 측정 또는 복사불가능성은 절대적인 통신보안을 보장할 새로운 암호방식을 제공한다.

절대 보안의 양자암호

양자암호기술은 도청이 불가능한 완벽한 암호기술로 불린다. 그래서 대다수 사람들에게는 공상과학소설에서나 가능할 것 같은 꿈의 암호기술로만 막연하게 느껴지고 있다. 하지만 놀랍게도 양자암호기술은 이미 현실이 되고 있다.

2005년 4월 21일 오스트리아 빈의 시장은 세계 최초로 양자암호 송금시스템을 이용해 빈대학의 짜일링거 교수에게 3천유로(약 4백만원)를 보냈다. 빈 시장은 양자암호연구에 써달라고 이 돈을 기부한 것이었다. 인터넷을 통한 은행거래에 비밀번호가 본인확인의 수단으로 쓰이고 있지만, 이 비밀번호가 인터넷 통신망을 통해 전달될 때에 제3자에게 도청당할 위험이 얼마든지 있다. 따라서 은행거래 등 여러 가지 중요한 통신을 할 때에는, 비밀번호를 컴퓨터에 입력하면 암호화되어 제3자가 읽더라도 알아보지 못하도록 보안시스템이 작동해야 한다. 양자암호 송금시스템은 비밀번호를 암호화하는 데에 사용한 비밀키(secret key)가 양자암호기술로 전송되었다는 의미이다.

그림 11. 고등과학원(KIAS)을 방문하여 강의하고 있는 IBM의 베넷 박사 : 베넷 박사는 1984년 양자암호기술을 발명하고, 1989년 양자암호기술 실험에 최초로 성공했으며, 1993년 양자텔레포테이션(양자원격전송)을 발명하였으며, 현재 양자통신 연구를 계속하고 있다.

한편 2005년 6월 3일에는 양자암호기술이 쓰인 컴퓨터 네트워크가 세계 최초로 가동되기 시작했다. 미 매사추세츠주 캠브리지시에 위치한 BBN 테크놀로지 사와 하버드대학 사이 약 10km거리에 걸쳐 양자암호기술을 사용하는 Qnet이라는 양자통신망이 개설된 것이다.

1984년 IBM의 베넷(Bennett) 박사와 몬트리올 대학교의 브라사드(Brassard) 교수가 양자암호기술을 발명했을 때만 하더라도 그냥 재미있는 이야깃거리 정도로만 생각되었다. 보통은 이론가들이 제시한 신기한 아이디어를 실험가들이 나서서 실험을 하게 마련인데, 이 아이디어는 실험가들의 이목을 별로 끌지 못했다. 그래서 이론가인 베넷 박사와 그 연구팀이 직접 나서서 1989년 세계 최초의 양자암호 실험을 성공시켰다. 그러나 이것 역시도 기존의 암호전문가들에게는 그렇게 깊은 인상을 주지 못했다. 기존의 공개키 암호기술이 워낙 든든해 보였기 때문이다. 그러나 1990년대부터 많이 연구되기 시작한 양자컴퓨터가 공개키 암호기술을 무력화시킬 수 있고, 절대적인 통신보안은 양자암호기술로만 보장된다는 인식이 퍼지면서, 양자암호기술이 급속히 발전하고 있다.

그렇다면 양자암호기술이란 대체 어떤 기술일까?

공개키 암호시스템 이전부터 쓰이고 있는 기존의 가장 안전한 암호시스템으로 일회용난수표 방식이 있다. 이 일회용난수표 암호시스템은 국가기밀의 전송, 외교채널, 스파이들의 통신 등에 현재 널리 쓰이고 있다. 두 통신당사자가 아무도 몰래 난수표를 나눠가질 수만 있으면 완

〈공개키 암호시스템과 양자컴퓨터〉

현재 인터넷 등 널리 사용되는 암호기술은 공개키 방식이다. 이 공개키 암호시스템이 양자컴퓨터의 등장으로 위협을 받고 있다.

비밀을 주고받고자 하는 사람들이 모두 똑같은 자물쇠를 갖고 있다고 하자. 그리고 오로지 열쇠를 가진 사람만이 이 자물쇠를 열 수 있다. 자물쇠를 잘 연구해보면 열쇠도 만들 수 있을 테지만, 아주 교묘하게 만들어진 자물쇠라면 거의 불가능할 것이다. 바로 이것이 공개키 암호시스템이다. 여기에서 자물쇠는 공개키, 열쇠는 비밀키에 해당한다. 이 상황을 수학적으로 비유해보면, 공개키인 자물쇠에 해당하는 것은 풀기가 거의 불가능한 아주 어려운 문제이고, 비밀키인 열쇠는 그런 문제의 해답에 해당한다.

실제로 인터넷통신에 쓰이는 공개키 암호시스템의 아주 어려운 문제는 큰 수의 소인수분해이다. 수십 자릿수의 소수 두개를 곱하여 만든 아주 큰 자연수가 공개키가 되는데, 이를 사용하여 메시지를 암호문으로 만든다. 이렇게 한 번 만들어진 암호문은 처음의 그 소수, 즉 비밀키를 알아야만 메시지로 변환시킬 수 있다.

이렇게 큰 수의 소인수분해를 이용하는 공개키 암호시스템은 1970년대에 리베스트(Rivest), 샤미르(Shamir), 에이들먼(Adleman) 세 사람이 발명했다. 이들이 세운 RSA 보안회사는 아직도 많은 돈을 벌어들이고 있다.

자신들이 만든 공개키 암호시스템의 보안성을 자신하던 RSA 세 사람은 1977년 Scientific American에 자신들이 만든 129자릿수의 자연수를 소인수분해하면 100달러를 주겠다는 현상문제를 발표하였다. 리베스트는, 1초에 10억번의 연산을 하는 컴퓨터를 쓰더라도 (실제 이런 컴퓨터는 1990년대에나 출현했다), 4 경(京 = 10의 16제곱) 년이 걸릴 것이라고 예측했다. 그러나 이 문제는 전세계 25개국 600여명의 자원자들이 1,600 여대의 각종 컴퓨터를 동원하여 8개월 동안 계산한 끝에 1994년 4월 2일에 풀리고 말았다. 그러나 여전히 소인수분해는 숫자의 자릿수에 거의 지수함수 정도의 시간이 소요되는 어려운 문제이다.

공개키 암호시스템에 적신호가 켜진 일은 바로 양자컴퓨터의 등장이었다. 1994년 미국의 유명한 통신회사인 AT&T의 피터 쇼어(Peter Shor) 박사가 양자컴퓨터를 써서(자릿수의 세 제곱 정도에 비례하는) 아주 짧은 시간 내에 소인수분해를 할 수 있는 양자알고리듬을 고안해낸 것이었다. 아직 본격적인 양자컴퓨터가 만들어지지는 않았지만, 양자컴퓨터는 디지털컴퓨터로서는 거의 불가능에 가까운 계산들을 순식간에 해치울 것으로 기대되고 있다. 따라서 '아주 어려운 문제'에 그 보안성을 의존하는 공개키 암호시스템은, 양자컴퓨터 앞에 언젠가는 무장해제가 될 운명에 처하게 된 것이다.

〈일회용난수표가 일회용이어야 하는 이유〉

일반 문자의 암호화는 우선 문자열을 이진수자 코드로 바꾸고, 거기에 이진수자 비밀키를 더한다. (이때에 덧셈은 이진수덧셈으로 0+0=1+1=0, 0+1=1+0=1 이 되고, 뺄셈은 덧셈과 똑같다.) 문자열 M1과 M2를 암호화하면서 같은 비밀키 K를 사용하여 암호문 E1과 E2를 얻었다고 하자. 각각의 암호문 E1이나 E2는 K를 모르는 한 해독할 수 없지만, 두 암호문을 더하면

$$E1 + E2 = (M1 + K) + (M2 + K) = M1 + M2 + K + K = M1 + M2$$

처럼 되어 비밀키의 흔적이 사라지고 그냥 두 문자열을 더한 것과 같아져서, 문자열을 추측할 가능성이 생긴다. (이진수 덧셈에서는 같은 수를 두 번 더하면 0이 된다.) 따라서 완벽한 보안을 위해서 일회용난수표는 한 번만 사용해야 한다.

벽한 암호통신을 할 수 있는 장점이 있다. 하지만 2가지 문제점이 있다.

그 하나는 아무도 몰래 두 사람만 이 난수표를 나눠가지기가 현실적으로 지극히 어렵다는 점이다. 난수표를 007가방에 넣어 배달하는 사람의 손목과 함께 수갑을 채워서 수많은 사람들이 감시하는 가운데에 전달하는 것을 영화 같은 데에서 볼 수 있지만, 그래도 누군가가 슬쩍 훔쳐낼 가능성이 항상 있는 것이다.

또 다른 문제점은, 이 난수표는 꼭 한 번만 사용해야 완벽한 암호통신을 유지할 수 있다는 것이다. 그래서 '일회용'이라는 접두어가 붙어 있는데, 똑같은 난수표를 써서 만든 암호문 두 개를 겹쳐 보면 암호문은 물론 난수표까지도 드러날 가능성이 있기 때문이다. 실제로 구소련의 스파이로 미국의 핵기밀을 훔치던 로젠버그 부부가 같은 난수표를 거듭 사용하는 바람에 발각되어 1953년에 처형된 일이 있다.

양자암호기술은 양자역학의 원리를 이용해 이런 문제점을 모두 해결해줄 수 있다. 아무에게도 도청되지 않고 계속적으로 난수표를 만들어내 완벽한 통신보안이 보장되는 것이다.

그렇다면 양자암호기술은 어떻게 이런 일을 구현해줄 수 있을까?

양자통신채널로 지나가는 양자정보를 도청하는 방법으로 두 가지를 생각해 볼 수 있다. 하나는 지나가는 양자정

〈양자정보의 복사불가능성과 양자측정의 비가역성〉

|a〉라는 양자정보를 복사하여 |a〉|a〉처럼 두 개가 될 수 있고, |b〉도 복사하여 |b〉|b〉처럼 된다고 하자. 양자정보 |a〉와 |b〉가 겹쳐진 상태 (|a〉+|b〉)를 복사하면, |a〉는 |a〉대로 복사되고 |b〉는 |b〉대로 복사되어 (|a〉|a〉+|b〉|b〉)가 된다. 이것은 복사 결과 (|a〉+|b〉)(|a〉+|b〉)를 얻으려는 것과 다른 결과가 된다. 또 양자정보의 복사가 가능하면 불확정성이론을 비롯한 양자물리학과 빛보다 빠른 통신이 불가능하다는 상대성이론 등 현대 물리학의 양대축이 무너진다.

수평편광|→〉은 직진통과시키고 수직편광|↑〉은 90도로 반사시키는 편광빛살가르개(polarizing beam splitter)에 수평편광과 수직편광이 중첩된 45도 편광의 단일광자 |↗〉를 통과시키면, 이 단일광자는 수평편광이 되어 직진통과하든지 아니면 수직편광이 되어 90도로 반사된다. 이렇게 하여 한 번 수평편광 또는 수직편광으로 측정된 것은 측정 이전의 상태가 어떤 상태였는지 알 수 없다.

보를 복사하는 것인데 이것은 양자정보의 복사불가능성 덕분에 피할 수 있다. 또 다른 하나는 지나가는 양자정보를 살짝 끄집어내어 측정해보고 다시 양자통신채널로 집어넣는 것이다. 이렇게 하면 측정 전과 후의 양자상태가 달라지므로 정식 통신당사자들이 몇몇을 정해서 어떤 상태를 보냈는데 어떤 상태로 받았는지 비교해보면 도청이 있었는지 또는 양자통신채널에 이상이 없는지 확인할 수 있다. 지나가는 양자정보를 도청자가 둘로 쪼개어 도청하는 것을 방지하기 위해 전송용 큐비트로 단일 광자(single photon)를 쓰는 것도 중요하다.

베넷과 브라사드가 발명한 양자암호방식 BB84에 대해서 좀더 자세히 알아보자. 갑돌이가 을순이에게 단일광자를 보내는데, →, ↑(⊕방식; 수평수직 편광방식), ↗, ↖(⊗방식; 대각선 편광방식) 등 네 가지 편광상태 중에서 하나로 만들어 보낸다. 이렇게 하기 위해 갑돌이는 각각 50% 확률로 0 또는 1이 나오게 하는 난수발생기(random number generator) 두 개를 사용한다. 첫 번째 난수발생기는 을순이에게 보낼 비트 0 또는 1을 결정하고, 두 번째 난수발생기는 이 비트를 코딩할 편광방식 ⊕방식 또는 ⊗방식을 결정한다.

예를 들어, 갑돌이의 두 난수가 0과 0이라면 비트 0을 ⊕방식으로 코딩하여 →편광의 단일광자를 을순이에게 보내게 된다. 01은 0을 ⊗방식으로 코딩하여 ↗편광을, 10은 1을 ⊕방식으로 코딩하여 ↑편광을, 11은 1을 ⊗방식으로 코딩하여 ↖편광을 보낸다.

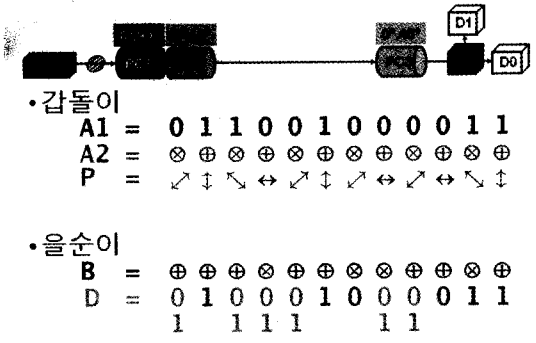

그림 12. BB84 양자암호전송. 갑돌이는 수평편광 단일광자를 발생시킨 후, 첫 번째 난수가 0이면 0도, 1이면 90도 포켈쎌을 이용하여 편광을 회전시키고, 두 번째 난수가 0이면 0도, 1이면 45도 편광을 회전시킨 후 을순이에게 보낸다. 을순이는 난수가 0이면 0도, 1이면 -45도 편광을 회전시킨 후, 편광 빛살가르개(polarizing beam splitter)를 사용하여 측정한다. 편광 빛살가르개는 수평편광은 그대로 통과시키고 수직편광은 반사시켜 90도로 진행경로를 꺾어 보낸다. 갑돌이가 보낸 편광방식과 을순이가 읽는 편광방식이 같으면, 두 사람의 비트는 항상 같게 된다.

을순이도 난수발생기를 사용하여, 0이 나오면 ⊕방식, 1이 나오면 ⊗방식으로 갑돌이가 보내온 단일광자의 편광을 측정한다. 을순이의 편광 측정 결과가 → 또는 ↗이면 을순이는 갑돌이가 보낸 비트를 0으로 해석하고, ↑ 또는 ↖이면 1로 해석한다.

갑돌이가 보낸 편광방식과 을순이가 측정하는 편광방식이 같으면, 갑돌이가 보낸 비트와 을순이가 해석한 비트는 똑같은 것이 되고, 두 사람의 편광방식이 다르면 두 사람의 비트는 50%의 확률로 같을 수도 있고 다를 수도 있다. 예를 들어, 갑돌이의 난수쌍이 01이면 갑돌이는 ↗편광을 보낸다. 이 때에 을순이의 난수가 1이라서 갑돌이와 똑같은 편광방식인 ⊗방식으로 측정하면 100%의 확률로 ↗편광을 얻게 되고, 을순이는 이를 갑돌이가 보낸 비트와 같은 0으로 해석하게 된다. 그렇지만 을순이의 난수가 0이라면 을순이는 ⊕방식으로 측정하게 되는데, ↗편광은 ⊕방식으로 측정할 때에 50%의 확률로 →로 측정되기도 하고 ↑로 측정되기도 한다. 을순이는 이를 0 또는 1로 해석하게 되어, 갑돌이가 보낸 비트를 맞출 확률이 50% 밖에 되지 않는다.

두 사람 사이의 단일광자 전송이 끝나면, 두 사람은 보낸 상태나 읽은 상태, 즉 비트는 공개하지 않고, 보낸 방식과 읽은 방식만을 공개적으로 비교한다. 갑돌이가 보낸 방식과 을순이가 읽은 방식이 같으면 두 사람은 똑같은 양자상태를 인식하게 되므로 이를 이용하여 일회용난수표를 만들면 된다.

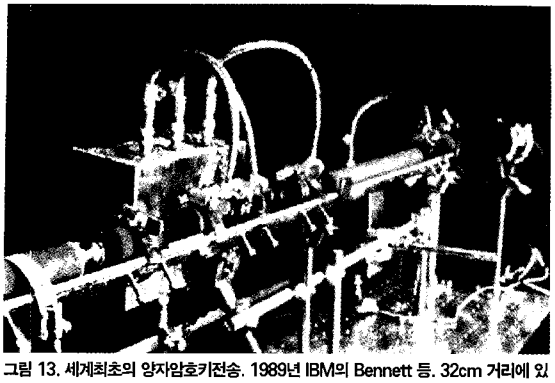

그림 13. 세계최초의 양자암호키전송. 1989년 IBM의 Bennett 등. 32cm 거리에 있는 두 송수신 장치 사이에 4가지 편광 상태를 이용한 양자암호키전송을 성공시켰다.

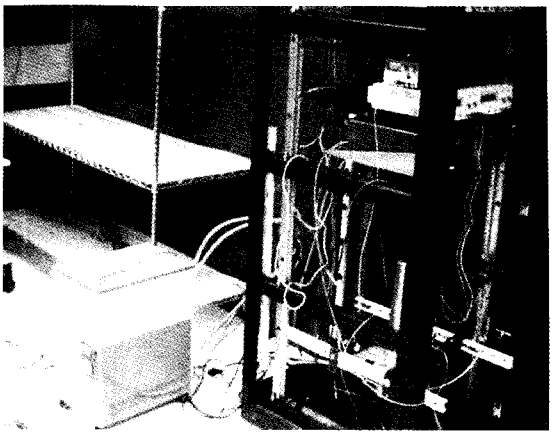

그림 14. 저온초전도체로 만들어진 초고속 광자검측기를 사용한 양자암호 송수신 장치: BBN Technology, 2006년 3월.

앞에서 말한 대로 양자통신채널을 도청하기 위해 통신채널로 지나가는 양자상태를 복사하는 것은 불가능하다. 또 다른 도청방식으로 도청자가 중간에서 양자상태를 읽는다면, 갑이 보낸 편광방식과 을이 읽는 편광방식은 같고 도청자의 편광방식만 다르다면, 50%의 확률로 같아야 할 갑돌이와 을순이의 비트가 달라지게 된다. 따라서 갑돌이와 을순이는 두 사람의 편광방식이 같은 것들 중에서 몇몇을 골라 정말로 두 사람의 비트가 같은지 확인해 봄으로써 도청여부를 가늠해 볼 수 있다. 서로 다른 경우가 너무 많으면 통신채널의 이상이나 도청가능성을 의심해보아야 한다. 보낸 방식과 읽는 방식이 다를 경우에는 두 사람이 인식하는 양자상태 사이에 아무런 상관관계가 생기지 않으므로 무시한다.

1989년 세계 최초의 양자암호실험에서 네 가지 편광 중 하나로 코딩된 단일광자는 32cm를 날아가서 검측되었다. 이후 양자암호기술의 실용화를 향한 경쟁에 불이 붙어 여러 가지 방식의 양자암호기술들이 속속 개발되고 있다. 일본 기업인 미쯔비시와 도시바가 2003년에 각각 80km, 100km 광섬유 양자암호통신에 성공했다고 발표했다. 스위스 제네바 대학교의 지생(Gisin) 교수가 세운 벤처기업 id Quantique社(www.idquantique.com)에서는 2002년에 제네바와 로잔 사이의 67km 광섬유를 통한 양자암호통신에 성공한 제품을 판매중이고, 미국의 벤처기업인 MagiQ Technology社(www.magiqtech.com)도 2004년 6월 현재 120km 광섬유 양자암호통신을 할 수 있는 Navaho라는 제품을 팔고 있다. Navaho라는 이름은 제2차세계대전 중 미국의 암호통신에 인디언언어를 활용한 미국인디언부족의 이름에서 따온 것이다. 단일광자가 광섬유를 통해서 흡수되거나 상태가 변하지 않고 전달될 수 있는 최대거리가 약 120km에 달한다고 하니 거리상으로는 그 한계에 도달한 셈이지만, 대도시 내부 또는 가까운 도시들 사이의 양자암호통신은 충분히 할 수 있는 실용기술이 되는 셈이다. 최근 BBN Technology 사는 저온초전도체를 이용해 광자의 검측 속도를, 고체소자의 몇 kbps에 비해, 100Mbps 수준으로 획기적으로 증가시켰다.

국내 양자암호 실험 연구로는 전기연구소와 한국과학기술원에서 진행된 바 있으며, 최근 한국전자통신연구원(ETRI)과 고등과학원(KIAS)의 공동연구로 25 km에서 양자암호키를 전송하고 이를 AES(Advanced Encryption System)의 키로 활용하는 실용적인 양자암호실험이 2006년에 수행되었다.

양자암호기술을 광섬유통신뿐 아니라 위성통신에도 적용하려는 실험이 진행중이다. 현재 영국 브리스톨 대학교에서 연구하고 있는 래러티(Rarity) 교수팀은 2001년 23.4km 떨어진 알프스 산맥의 두 봉우리 사이에서 무선 양자암호통신에 성공하였다. 또한 원자탄을 개발한 곳으로 유명한 로스알라모스 미국국립연구소의 휴즈(Hughes) 박사팀은 2002년 대낮에 10km 무선 양자암호통신에 성공함으로써 저궤도 위성암호통신의 가능성을 보여주었다. 햇빛이 내리쬐는 대낮에 대기 중에서 이런 실험에 성공했다는 것은 대단한 의미가 있다. 태양으로부터 쏟아져 내리는 엄청나게 많은 광자가 대기 중에서 산란되어 흩어지면서 양자암호통신에 쓰이는 광자들과 뒤섞일 가능성이 높기 때문이다. 광섬유는 광자를 정확히 원하는 곳까지 전해주는 통로역할을 하지만, 대기

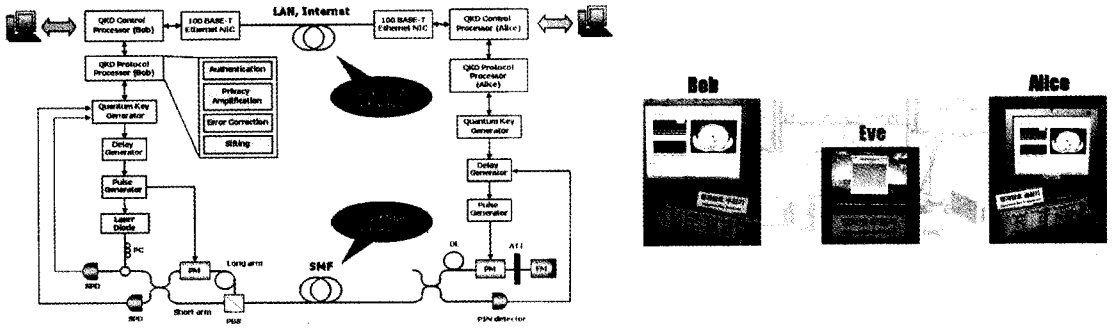

그림 15. 한국전자통신연구원(ETRI)과 고등과학원(KIAS)의 양자암호 실험 (25km, 2006년 12월)

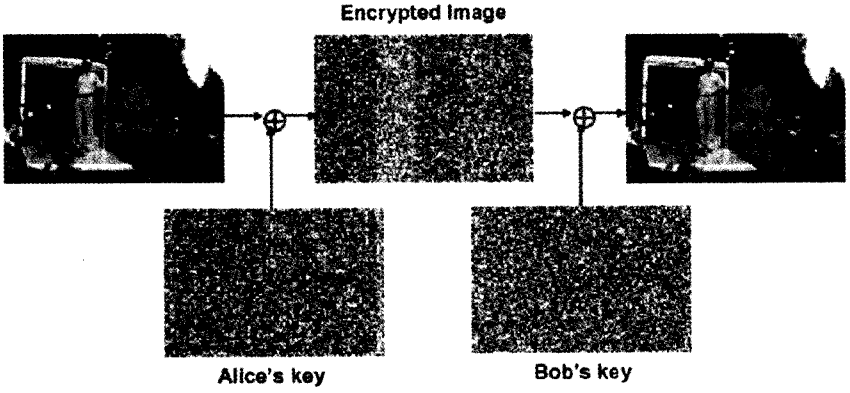

그림 16. 로스알라모스 휴즈박사팀의 대기 중 양자암호 실험

중 실험에서는 수십km떨어진 두 지점이 서로를 정확히 겨냥해야 하고, 광자가 대기중의 공기분자와 충돌하여 사라지는 것도 고려해야 한다. 호주도 2002년부터 국가 차원의 양자암호통신연구에 무선양자암호통신을 포함시키고 있다. 위성양자암호통신이 가능하게 되면 광섬유양자암호통신이 가진 거리의 제한을 넘어서 전지구 양자암호통신망을 구축할 수 있게 된다.

앞에 인용한 양자암호기술 두 가지는 기술적으로 매우 중대한 진전이다. 단일광자 양자암호기술에 거리 제한이 있는 것과 달리, 짜일링거 교수 연구팀의 양자얽힘을 이용한 양자암호기술은, 양자텔레포테이션 또는 양자원격전송을 이용하는 양자중계기를 둘 수 있어서 전송거리에 제한이 없는 유선 양자암호통신의 첫걸음이라는 점에서 중요하다.

Qnet은, 이전까지의 양자암호기술 실험이 두 지점 사이에서만 진행된 데에 비해, 한 통신망상의 여러 통신당사자들 사이에서 양자암호기술을 실험한 것이다. 예를 들어, 100명이 양자암호통신을 하기 위해 둘씩 묶으면 양방향 양자암호통신채널 4950(=100×99/2)개가 필요하지만, Qnet 방식을 이용하면 이것들을 하나의 양자통신망으로 대체할 수 있기 때문에 실용성이 매우 높다.

이처럼 양자암호가 기술적으로 빠른 진보를 거두고 있는 데는 그만큼 세계적으로 이에 대한 관심이 높기 때문이다. 중요한 사실은 기술적 진보를 재촉하는 상황에 처해있다는 것이다. 재미있게도 양자컴퓨터의 등장으로 양자암호는 선택이 아니라 필수가 되고 있는 현실이다.

미국의 국가안보국 NSA는 수많은 음모론의 중심에 서 있는데, 그 중의 하나가 에셜론(Echelon)이라는 프로젝터를 통해 세계의 모든 통신을 엿듣고 있다는 것이다. 이것이 현실적으로 가능한 일인지는 알 수 없지만, 공개키 암호시스템으로 암호화되어 있는 암호문은 엿듣는다고 하더라도 그 메시지를 현재의 기술로 해독할 수는 없다.

그렇지만 이 암호문들을 계속 모아두었다가 멀지 않은 미래에 양자컴퓨터가 만들어지면 암호해독을 할 수 있을 것이다.

요즘 양자정보 관련 국제학회에 NSA는 연구원을 한두 사람씩 파견하고 있다. 미국의 통신보안을 위해 양자암호기술을 개발하는 것과 남들의 공개키 암호통신을 해독하기 위해 양자컴퓨터를 개발하는 것이 NSA의 공공연한 목표가 되고 있다. 공개키 암호시스템의 메카 RSA연구소의 연구책임자인 칼리스키(Kaliski) 박사는 양자암호기술을 "암호기술의 주요한 패러다임 변혁"이라고 하면서, "기존암호기술과 양자암호기술의 결합은 더욱 안전한 통신체계를 실현하는 강력한 도구"라고 말하고 있다. 현재 세계적으로 매년 약 5천만불 규모의 양자암호관련 연구가 진행 중인 것으로 알려져 있다.

이웃 일본에서는 매년 양자암호 및 양자정보관련 국제학회가 둘 셋 이상씩 열리고 있으며, 물리학자들뿐 아니라 컴퓨터 및 정보전공의 학자들이 대거 참여하고 있다. 이에 비해 우리나라는 아직 얼마되지 않는 물리학자들과 수학자들만이 관련 연구를 하고 있는 실정이고, 정보통신사업 분야의 기업적인 투자는 전무한 형편이어서 현재의 정보통신강국이라는 명성을 어떻게 이어갈 수 있을지 염려스럽다. 또한 우리나라 정보보안의 취약성을 극복하고 정보의 국제경쟁에서 정보보안주권을 확보하기 위해서라도 양자암호기술에 대한 투자가 필요하다. 양자암호기술은 가장 기초적인 양자정보기술로서, 앞으로 양자컴퓨터를 비롯한 다른 양자정보기술의 토대가 된다. 양자정보과학분야의 연구는 아직 역사가 길지 않아서 우리가 얻을 기회도 많이 있어 보인다.

참고문헌

[1] Pieter Kok et al., quant-ph/0512071 v.2 (2006.3.14) "Linear optical quantum computing."

[2] C. R. Myers and R. Laflamme, quant-ph/0512104 (2005.12.13) "Linear optics quantum computation: an overview."

[3] E. Knill, R. Laflamme, and G. J.Milburn, Nature 409, 46 (2001).

[4] R. Raussendorf and H. J. Briegel, Phys. Rev. Lett., 86 5188 (2001) and R. Raussendorf, D. E. Browne, and H. J. Briegel, Phys. Rev. A, 68 022312 (2003).

[5] H. Lee and J. Kim, Phys. Rev. A 63, 012305 (2001).

[6] "Optical Approaches to Quantum Information Processing and Quantum Computing" (2002) available at "http://qist.lanl.gov/pdfs/optical.pdf".