양자 정보통신 기술 동향과 시사점

Trends of Quantum Information & Telecommunication Technology

이성용(S.Y. Lee) 정보체계연구팀 연구원
정현수(H.S. Chung) 정보체계연구팀 책임연구원, 팀장

본 고에서는 최근 IT-NT 융합 기술 중 각광받고 있는 양자 정보통신 기술의 기초 이론 및 최신 동향 그리고, 실제적인 시스템 구현을 위한 구성 요소들을 살펴보고자 한다. 양자정보통신 기술은 광자(光子)의 양자역학적 특성에 기반을 둔 기술로서 양자 이론과 밀접한 관련을 가진 기술 분야이다. 일반적으로 양자정보처리 기술은 크게 양자 컴퓨터(quantum computer)와 양자 암호화(quantum cryptography) 기술, 양자 통신(quantum communication) 등으로 구분된다. 양자정보통신의 각 분야 기술이 아직은 기초연구 수준에 있지만 세계적으로 그 중요성을 인식하고 대규모 투자를 아끼지 않는 분야이기 때문에, 이 분야에 대한 투자를 소홀히 하면 기술 종속 또는 기술 후진국으로 전락할 수도 있다. 그러므로, 본 고에서는 외국의 기술 발전 추세에 대처하고 자체적인 관련 기반 기술을 확보하기 위한 기초 이론과 기술 동향에 대해 간략히 살펴보기로 한다.

I. 서 론

나노(nano) 기술은 바이오 기술(BT)과 더불어 정보기술(IT)과 융합하여 미래 유망기술 발전의 촉매역할을 하고 있으며, 기존 기술의 한계를 극복할 수 있는 대안으로 부상하면서 선진 각국 및 우리나라의 국가경쟁력 확보를 위한 전략 분야로 육성하고 있으며, 이를 이용하여 정보통신 분야의 한계를 극복해 보고자 하는 연구도 활발히 진행중이다.

최근 대규모 집적회로(VLSI) 기술의 비약적인 발전에 힘입어 보다 많은 정보를 더 신속하게 처리하게 할 수 있게 되었으며, 이를 위한 근간으로는 무엇보다 필수적으로 집적화 기술이 요구되었다. Moore 법칙에 의하면, 집적회로에 들어가는 트랜지스터의 수는 약 18개월마다 두 배로 증가한다고 하며, 이 법칙에 따르면 2020년경에는 칩의 고집적화로 인해 표면전기장(surface electronic field)의 증가로 potential well에 의한 양자현상을 피할 수 없는 상황에 도달하게 된다고 한다[1].

또한, Robert Kyeses가 연구한 정보 저장에 필요한 전자의 수를 시간의 흐름에 대해 분석한 자료에 따르면, 향후 20년 후면 1개의 원자에 1개의 비트를 저장할 수 있는 수준에까지 도달할 수 있을 것이라 한다[2].

이렇게 머지않아 우리생활에 직접 이용될 양자현상을 이해하고, 양자계가 갖는 독특한 성질을 이용하고자 하는 연구가 증대되고 있다. 특히, 현재보다 여러 가지 면에서 발전된 정보처리가 가능하다는 이론에 따라 정보처리 및 통신 분야에 양자역학을 적용해 보려는 연구가 많이 성행하고 있다.

현재 컴퓨터에서 사용되는 정보의 최소 단위인 비트(bit)는 0 또는 1 중 한 값을 갖게 되고 이를 정보처리에 이용하지만, 양자 역학을 활용하면 상태가 겹치는 중복상태로 존재할 수 있기 때문에 0 또는 1

의 두 가지 값을 가질 수 있을 뿐 아니라 0과 1을 동시에 지닐 수도 있다. 이를 컴퓨터에 활용하면 획기적인 병렬처리를 수행할 수 있게 되는 것이다.

암호학 분야에 양자이론을 적용하는 것은 많은 진전을 보여주고 있다. 이는 양자계의 성질을 이용하여 정보를 전송할 때, 제 3자가 도청을 시도하면 필연적으로 전송된 정보에 잡음이 들어가게 되는 성질을 이용한 것이다. 즉, 전자에 대한 Young의 이중슬릿 실험에서 슬릿의 한 쪽에서 전자를 측정하면 간섭무늬가 사라지는 것과 비슷한 효과를 응용한 것이다[3].

또 다른 예로서 양자전송을 들 수 있다. 얽혀있는 두 입자를 이용하면 큐빗을 전송할 수 있는데, 이를 이용하면 미래의 양자 컴퓨터간 큐빗의 교환 혹은 큐빗의 저장장치의 원리로 사용할 수 있다[4].

본 고에서는 이러한 양자의 특성을 정보처리 기술에 활용한 사항을 크게 양자 컴퓨터, 양자 암호화 기술, 양자 통신 기술로 구분하여 살펴보고 앞으로의 전망을 간략히 점검해 보고자 한다.

II. 양자 컴퓨터

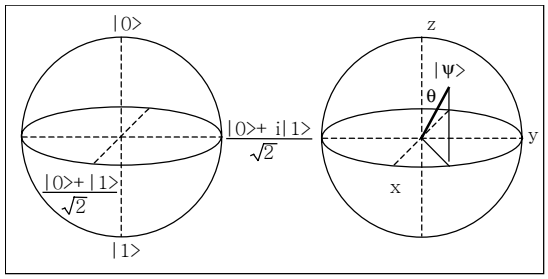
양자 컴퓨터 기술을 활용하면, 하나의 연산 작업에 대해 많은 양자 상태의 정보를 동시에 처리할 수가 있어 대용량 정보처리가 용이하다.

기존 컴퓨터의 크기를 최소화하는 데 가장 큰 문제는 생성되는 열을 어떻게 처리하느냐이다. 1961년에 란다우는 열의 발산에 기초한 컴퓨터의 물리적 한계를 연구하였다. 그는 계산에 필요한 거의 모든 오퍼레이션들이 가역적(reversible)으로 실행될 수 있음을 보일 수 있었으며, 이는 곧 열을 발산하지 않고 실행될 수 있는 것을 의미한다. 어떤 장치가 가역적이기 위한 첫번째 조건은 그것의 입력과 출력이 어느 쪽에서도 서로 검색 가능해야 한다. 이것을 "논리적 가역성"이라 한다. 논리적 가역성 뿐만 아니라 디바이스가 거꾸로 실행될 수 있다면 "물리적 가역성"이라 부르고 그렇게 되면 열역학 제2법칙에 의해 열을 발산하지 않게 된다. 이러한 classical, reversible computation의 연구결과는 양자컴퓨터 개발의 기초가 되었다[5]-[7].

기존의 컴퓨터에서 비트가 정보를 표현하는 기본단위라 말한다면, 양자컴퓨터에서는 큐빗(quantum bit, qu-bit)이 정보를 표현하는 기본단위이다. 큐빗으로 표현되는 정보는 2차원 힐버트 공간(hilbert space)에 존재하는 상태 벡터를 이용하여 다음과 같이 표현될 수 있다((그림 1) 참조).

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \qquad (1)$$

여기서 α와 β는 임의의 복소수이며, 상태벡터의 정규화(normalization) $|\alpha|^2 + |\beta|^2 = 1$을 만족한다. 고유벡터 |0>과 |1>은 기존 컴퓨터의 비트 {0,1}에 대응되는 2차원 힐버트 공간의 직교정규화 기저이다. 실제로, 일반적으로 물리계에 양자화된 두 상태가 존재한다면, 이들 중 한 상태를 |0>, 나머지 한 상태를 |1>로 놓고 그 계를 큐빗으로 사용할 수 있다[8].



(그림 1) 큐빗의 표현

여러 개의 큐빗을 모아 놓은 그룹을 레지스터라 한다. 만약 n개의 큐빗이 모였다면 이 레지스터를 기술하기 위해선 2^n 차원의 힐버트 공간이 필요하고, 전산기저는 |00…0>, |10…0>, |11…0>, |11…1>로서 2^n 개가 존재한다. 여기서, |00…0>은 레지스터를 구성하는 모든 큐빗이 |0> 상태에 있음을 의미하며, 이들 각각의 상태가 다음과 같이 결합되어 있는 것이다.

$$|00\Lambda\ 0\rangle = |0\rangle \otimes |0\rangle \otimes \Lambda\ |0\rangle \qquad (2)$$

레지스터의 상태는 이들 전산 기저들간의 중첩상태도 허용한다. 이러한 중첩상태는 n=2일때 다음과

같은 EPR쌍도 포함된다.

$$|\psi_{EPR}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \quad (3)$$

특히, 이러한 상태를 얽힘(entangled state)이라고 하며, 양자 암호화와 양자 통신에서 중요하게 사용된다. 양자 컴퓨터로 함수 계산을 위해서는 입력 단자와 출력 단자에 각각 두 개의 레지스터가 필요하다. 준비된 두 개의 레지스터를 이용하여 함수의 값을 계산하려면 다음과 같은 유니터리 작용소인 함수 계산 작용소(function evaluation operator)를 사용한다.

$$U_f : |x\rangle \otimes |y\rangle \rightarrow |x\rangle \otimes |y + f(x)\rangle \quad (4)$$

일반적으로, 이 함수 계산 작용소 U_f 는 함수 값 하나하나를 계산하는 것이 아니라 중첩된 상태로 모든 입력에 대한 함수 값을 한 번에 계산할 수 있다. 이를 통해서 자연스럽게 양자 병렬처리(quantum parallelism)를 수행한다[9].

기존 컴퓨터에서는 8비트 연산을 위해서는 CPU 등을 바탕으로 기본 게이트들을 공간적으로 잘 조합하여 배열하지만, 양자컴퓨터에서는 8개의 큐빗입자들의 모임인 레지스터가 전부이다. 이 8개의 큐빗에 8비트정보가 표현되고, 이 레지스터에 가해지는 유니터리 변환의 시간적 순서에 의해 원하는 연산을 수행할 수 있는 것이다. 현재까지 국내외에서 연구중인 양자컴퓨터 이론을 크게 4가지로 구분하여 정리해 보면 다음과 같다[10].

1. Photon Quantum Computer

포톤 양자 컴퓨터는 말그대로 광자를 소자로 이용하는 방식의 컴퓨터이다.

포톤의 분극이나 공간상의 위치를 양자화시켜 큐빗을 구현하고, 유니터리의 변환은 phase shifter, beam splitter, 또는 비선형 Kerr 효과를 이용하며 상태 벡터는 단광자를 발생시켜 얻는다.

단점으로는 크기가 크며, 비선형 Kerr 효과가 큰 배질을 찾기가 힘들다는 점이다.

2 . Cavity Quantum Electrodynamics

큐빗의 구현 방법은 3.1의 포톤 양자 컴퓨터와 동일하지만, 수 개의 원자가 구속된 Fabry-Perot QED Cavity를 phase shifter 및 beam splitter와 함께 양자게이트로 사용할 수 있다는 점이 다르며, 단점으로는 스케일링이 곤란하고 크기를 줄이기 힘들다는 점이다.

3. Ion Trap

이온 트랩방식은 인공으로 원자를 만들어 이용하는 방식으로, 트랩된 원자의 진동모드와 핵자기 상태를 큐빗으로 이용하며, 게이트의 역할은 레이저 펄스로 Jaynes-Cummings 상호작용을 유발시켜 원자의 상태를 제어한다. 단점으로는 진동모드의 수명이 극히 짧고, 이온의 기저상태를 만들기가 힘들다는 점이다.

4. NMR

분자의 수소고리에 있는 원자의 핵자기 스핀을 큐빗으로 이용하며, 외부에서 인가된 자장이 양자게이트의 역할을 한다. 현재 양자컴퓨터의 가능성을 보여주기 위해 가장 많이 연구된 분야 중의 하나로서, 단점으로는 순수한 상태를 만들기가 어렵고 스케일링이 거의 불가능하다는 점이다.

III. 양자 암호화 기술

1. 암호키의 분배문제

여러 암호학자들의 연구에 힘입어 전체 정보에 대한 보안성을 암호키 하나에 집중시키는 것이 가능해졌다. 암호키의 보안만 확보하면 전체 정보를 비밀리에 교환하는 일이 가능해진 것이다. 이러한 암호체계는 여러 가지가 있으나 공통적으로 암호키의 분배문제가 발생한다. 공개키 방법은 키분배 문

제를 수학적인 방법으로 해결하고자 한 예이다. 이 방법은 큰 수의 인수분해가 어렵다는 성질을 이용하고 있다. 현재 전자상거래에도 이용되고 있는 RSA 방법은 512비트의 공개키를 사용하고 있으나, 최근 효율적으로 인수분해를 하는 알고리듬과 컴퓨터의 발전에 힘입어 512비트로는 더 이상 안전하다고 할 수 없다는 의견이 지배적이다. 또한 양자컴퓨터 이론은 암호키의 비트 수를 늘려가는 것만으로는 보안성을 확보할 수 없음을 알려주고 있다. 양자암호화는 이러한 키분배 문제를 해결할 대안으로 생각할 수 있으며 현재 활발한 연구가 진행중인 분야이다.

2. 고전적인 암호화 방법-비밀키 방법

암호화 기법 가운데 one-time pad를 이용한 방법을 예로 들면 다음과 같다.

Alice와 Bob이 통신을 하려 하고 Eve가 중간에서 도청을 시도하는 상황을 고려해 보도록 한다. Alice와 Bob은 미리 안전한 방법을 통해 비밀키{K_1, K_2, ..., K_n}를 공유한다. 비밀키는 무작위 수열이며 보내려는 정보와 길이가 같다. (길이 n) Alice는 보내려는 정보에 비밀키를 더하는 방법으로 암호화한 다음 Bob에게 보낸다.

정보 : $\{M_1, M_2, ..., M_n\}$ (5)

암호화 :$\{E_1, E_2, ..., E_n\}$, $E_i = (M_i + K_i) \pmod L$ (6)

여기서 L은 정보를 구성하는 문자의 개수이며 L로 나누어 그 나머지를 취하는 과정(mod L)은 비밀키를 더했을 때 L보다 큰 수에 대하여 다시 L의 범위 안에 들어가도록 해주는 것이다.

Bob은 받은 정보에서 비밀키를 빼는 방법으로 정보를 복원하면 된다.

$\{M_1, M_2, ..., M_n\}$, $M_i = (E_i - K_i + L) \pmod L$ (7)

비밀키를 모르는 Eve는 무작위 수열을 가정해서 매번 일일이 해독을 시도해야 하므로, 정보를 알아내기가 거의 불가능하다.

위에서 예로 든 one-time pad를 이용한 방법은 정보의 길이와 비밀키의 길이가 같아야 하므로 비효율적이다. 또한, 이러한 비밀키를 이용하는 방법의 가장 큰 문제점은 비밀키를 분배하는 과정에서 Eve가 키를 몰래 복제하는 데 성공할 경우 암호가 깨졌다는 사실을 모르는 채로 모든 정보를 교환할 우려가 있다는 사실이다. 키복제를 막기 위해 여러 가지 물리적인 보조수단이 동원될 수 있으나 암호체계 전체의 비용을 늘여야만 가능하다. 따라서 전자상거래 등 멀리 떨어져 있는 여러 사람이 이용하는 경우에는 실용적이지 못해 다음에서 제시하는 공개키 방법을 주로 이용하고 있다.

3. 고전적인 암호화 방법-공개키 방법

이 방법은 비밀키와 함께 공개키를 이용해서 키분배 문제를 해결하는 방법이다. 현재 전자상거래에 사용되고 있는 RSA 암호체계의 기본을 살펴보면 다음과 같다.

Bob은 굉장히 큰 두 개의 소수 p와 q를 고른다. n=pq 와 m=(p-1)(q-1) 이라고 하면, d와 e는 다음과 같은 규칙에 의해 만들어진다.

d와 m은 서로 소 (8)

$e \times d \pmod m = 1$ 이 성립 (9)

(e, n)은 공개키, (d, n)은 비밀키가 된다. 공개키는 정보를 암호화 할 때에만 쓰이며 비밀키가 있어야만 암호를 풀 수 있다. 비밀키를 모르는 제3자가 암호체계를 깨기 위해서는 공개키의 e, n을 이용해서 d를 추측해야 하는데, 그러기 위해서는 n을 인수분해 하여 두 인수 p, q를 알아내야 한다. 이는 굉장히 큰 수의 인수분해를 해야 암호체계를 깰 수 있다는 말인데, 일반적으로 큰 수는 인수분해하기 힘들다는 수학적 알고리듬 복잡도를 활용한 방법이라 할 수 있다. Bob은 공개키 (e, n)을 공개하고, Alice는 (e, n)을 이용해서 정보를 다음과 같이 암호화한 뒤 Bob에게 보낸다.

$$E_I = M_i^e \pmod n \quad (10)$$

Bob은 받은 정보를 다음과 같이 복원한다.

$$M_I = E_i^d \pmod n \quad (11)$$

위와 같은 과정이 가능한 이유는 오일러 정리 때문이다. 오일러 함수 Ø(N)은 N보다 작고 N과 서로 소인 자연수의 개수를 나타내는 함수이며 다음과 같은 성질이 있다.

$$Ø(AB) = Ø(A)Ø(B),\ A, B는\ 서로\ 소 \quad (12)$$

$$Ø(N)=N-1,\ N은\ 소수 \quad (13)$$

오일러 정리에 의해

$$M_i^m = M_i^{(p-1)(q-1)} = M_i^{Ø(n)} == 1 \quad (14)$$

이 성립하고 ed = mk+ 1(k는 임의의 정수)이므로,

$$E_i^d==(M_i^e)^d=M_i^{ed}=M_i^{mk} + 1==M_I \quad (15)$$

이 방법에서는 비밀키를 교환할 필요가 없으므로 여러 사람이 사용하는 전자상거래와 같은 경우에 매우 실용적인 방법이 된다. 그러나 이 기법은 큰 수의 인수분해가 어렵다는 전제 하에 생성한 알고리듬으로 만약 획기적인 인수분해 알고리듬이 발견된다면 그에 따라 큰 영향을 받을 수 있다. 또한, 컴퓨터의 성능이 계속 향상되더라도 키의 비트 수를 계속적으로 늘이면 된다는 전략 또한 양자컴퓨터의 병렬처리를 이용하면 쉽게 깨질 수 있다는 단점이 있다. 이러한 공개키 방법에서 사용하는 큰 소수는 아무나 찾을 수 있는 것이 아니므로 특정 소수 생성에 대한 문제를 선행하여 해결해야 한다는 것도 고려해야 할 사항이다.

4. 양자키 분배를 이용한 암호화 방법

양자물리의 간섭현상을 이용하면 위에서 제시한 문제점을 해결하고 안전하게 키를 교환할 수 있다.

양자정보는 복사가 불가능하다는 성질과 양자측정은 비가역성을 가진다는 성질로 인해 절대적인 보안이 보장되는 양자암호기술, 즉 양자암호키의 생성 및 전송방법이 고안되었다((그림 2) 참조).

현재 제안된 양자암호키 분배방법으로는 BB84, B92, EPR 프로토콜 등이 있다.

가. BB84 방식

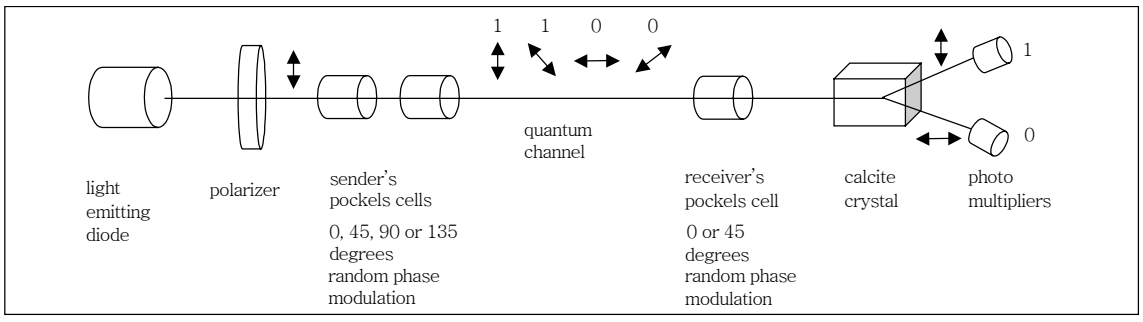
동시에 측정할 수 없는 두 개의 상태를 이용한 방법으로서 광자의 편광을 이용하며, 이를 위해서는 개별적인 광자의 편광상태를 제어하고 검출하는 기술이 필요하다.

1984년 IBM의 Bennett과 몬트리올 대학교의 Brassard는 단일광자의 편광을 이용한 양자암호키 생성 및 전송 프로토콜을 제안하였다((그림 3) 참조).

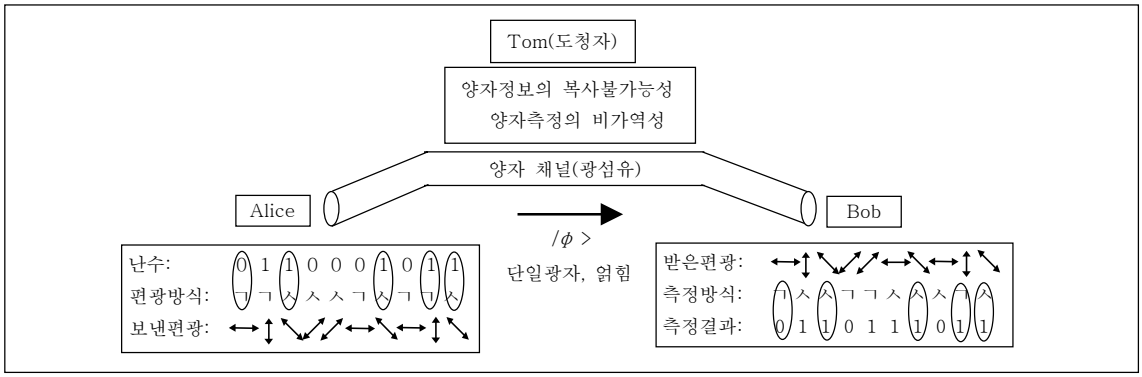
만약 도청을 하기 위해 양자통신채널로 지나가는 양자정보를 복사하려 한다면, 이 방법은 양자정보의 복사불가능성 때문에 불가능하다.

한편, 양자정보의 복사불가능성은 단일양자상태에 대한 것이므로, 양자암호체계를 만들기 위해서는 단일광자를 생성하는 것이 매우 중요하다.

만약, 양자통신채널을 잘라서 지나가는 양자정보



(그림 2) 양자 암호키 전송 흐름



(그림 3) BB84 방식의 양자암호키 전송

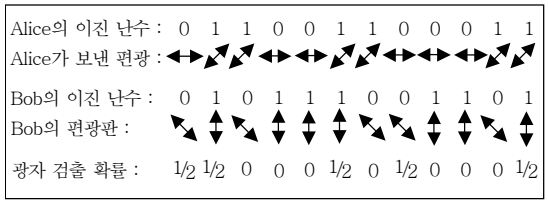
(1) Alice는 Bob에게 보낼 0과 1의 이진법 난수열을 만들어 'ㄱ 방식'={↔=0, ↕=1} 또는 'ㄴ 방식'={=0, =1}의 두 방식을 랜덤하게 섞어서 전송한다.
(2) Bob은 Alice가 보낸 단일광자의 편광을, ㄱ 또는 ㅅ 방식을 랜덤하게 섞어서 측정한다.
(3) 전송과 측정이 끝난 후, Alice와 Bob은 보낸 편광방식과 측정한 편광방식을 공개된 채널을 통해 비교한다.
(4) 두 사람의 편광방식이 같으면 두 사람이 보내고 받은 편광은 일치할 것이고, 이에 해당하는 이진수열도 같게 되므로 이들을 택한다.
(5) 이렇게 택한 이진수열 중 일부만 서로 공개하여 정말로 같은지를 확인한다.
(6) 만약 비교된 이진수열이 일치하지 않으면, 양자통신채널의 신뢰도가 떨어지든지 누군가가 도청을 한 것으로 간주할 수 있다. 양자암호키 생성 및 전송을 새로이 한다.
(7) 공개된 이진수열이 어느 정도 이상의 비율로 일치하면, 공개되지 않은 이진수열 부분을 암호키(일회용 난수표)로 삼으면 된다.

<양자암호키 생성 및 전송 프로토콜>

를 꺼집어내어 측정하고 다시 채널로 집어 넣는다면, 양자측정의 비가역성 때문에 Tom(도청자)이 한 번 측정한 양자정보의 상태는 더 이상 원래의 양자상태가 아닐 수 있다. 따라서 Alice와 Bob이 같은 편광방식으로 보내고 측정했다 하더라도 서로 다른 이진수를 가질 수 있다. Alice와 Bob은 이진수열 중 공개된 부분이 같은지를 비교하여 도청여부를 확인할 수 있는 것이다.

나. B92 방식

1992년 Bennett은 좀더 간단한 방식의 양자암호체계를 발표하였다((그림 4) 참조). Alice는 Bob에게 보낼 0과 1의 이진난수열을 만들고, 0은 ↔, 1은 ↗의 편광을 보낸다. Bob도 나름대로의 이진난수열을 만들어, 0은 ↖, 1은 ↕의 편광판으로 측정을 한다. Alice와 Bob의 이진수가 같은 50%의 경우에



(그림 4) B92 방식의 양자암호키 전송

편광과 편광판이 45도 겹치므로, 50%의 확률로 단일광자를 검출할 수 있다. 두 사람의 이진수가 다를 경우에는 편광과 편광판의 방향이 수직이 되어서 Bob은 광자를 검출할 수 없다. 따라서 이 방식으로는 전체적으로 25%의 확률로 Bob이 단일광자를 검출하게 되고, 이들 경우만 Bob이 Alice에게 알림으로써 두 사람은 같은 이진난수열을 가지게 된다. 또한, 두 사람은 BB84에서처럼 공개된 채널을 통해 일부 데이터를 비교함으로써 채널의 신뢰도 및 도청

여부를 판별할 수 있다.

IV. 양자 통신

양자원격이동(quantum teleportation)은 "모르는 양자상태의 공간 이동"이라 정의할 수 있다. 일반인은 아마도 양자원격이동이라 하면 사람 또는 물체가 왼쪽에서 오른쪽으로 또는 지구에서 화성으로 즉각적으로 옮겨가는 모습을 상상할 것이다. 그러나 물리학에서 현재 우리가 이해하고 있는 양자원격이동은 물체가 실제로 움직이는 것이 아니고 단지 한 입자의 상태가 공간상 떨어져 있는 다른 입자로 전이되는 현상을 말한다.

사실상 우리가 잘 알고 있는 팩스는 이러한 기능을 수행하고 있으며, 따라서 거시세계에서는 고전상태의 원격이동이 이미 수행되고 있다고 볼 수 있다. 그러나 양자세계에서는 상황이 달라 어떤 입자의 양자상태에 관한 정보는 측정을 통하여 얻어지지만, 그 양자상태에 관한 사전 지식이 없다면 그 상태에 관한 완전한 정보를 얻는 것은 일반적으로 불가능하다.

모르는 양자상태에 대한 완전한 정보를 얻는 것이 사실상 불가능한 상황에서 그 상태를 공간적으로 고스란히 전이시키는 방법을 제공해주는 것이 양자원격이동이고 그렇기 때문에 양자원격이동이 학문적으로도 흥미있는 현상이 되는 것이다.

양자세계에서는 복사불가원리에 의해서 모르는 상태를 완전히 복사하는 것이 불가능하다. 고전세계에서는 어떤 정보를 전달하기 위해서는 단순히 그 정보를 복사해서 복사본을 보내면 된다. 그러나 양자세계에서 모르는 양자상태가 완전히 이동되려면 송신장소의 상태는 깨질 수 밖에 없고 그 상태가 대신 수신장소에서 나타나는 형태가 되어야 한다. 이것이 바로 양자원격이동의 형태이며, 양자세계에서 모르는 상태에 관한 정보전달의 방법이 되는 것이다.

1. 얽힘

얽힘이란 입자들끼리 상호작용 후에 상태들이 서로 연관되어서 한 입자에 대한 측정이 그 입자 뿐 아니라 다른 입자들의 상태에도 영향을 주게 되는 현상을 말한다[11].

예를 들어 두 광자 A, B가 항상 서로 수직인 편광상태에 있다는 상관관계를 가지고 있으면, 광자 A가 수직편광이면 광자 B는 반드시 수평편광이고 광자 A가 수평편광이면 광자 B는 반드시 수직편광일 것이며, 이러한 두 광자의 편광상태는

$$|\psi\rangle_{AB} = \frac{1}{\sqrt{2}}(|\beta\rangle_A|\leftrightarrow\rangle_B + |\leftrightarrow\rangle_A|\beta\rangle_B) \quad (16)$$

로 표시된다. 여기서 $|\updownarrow\rangle_A$와 $|\leftrightarrow\rangle_A$는 각각 광자 A가 수직과 수평의 편광상태에 있음을 의미한다. 반대로 두 광자가 항상 서로 같은 편광상태에 있다는 상관관계를 가지고 있으면 두 광자의 편광상태는

$$|\psi\rangle_{AB} = \frac{1}{\sqrt{2}}(|\beta\rangle_A|\beta\rangle_B + |\leftrightarrow\rangle_A|\leftrightarrow\rangle_B) \quad (17)$$

로 표시된다. (16) 또는 (17)의 상태가 얽힘상태의 예가 된다[10]. 얽힘의 개념은 물론 광자의 편광상태에만 적용되는 것이 아니고 두 핵의 스핀, 두 원자의 상태 등에도 똑같이 적용된다. 예를 들어 두 원자 A, B가 원자 A가 아랫준위에 있을 때 원자 B는 반드시 윗준위에 있고 원자 A가 윗준위에 있을 때 원자 B는 반드시 아랫준위에 있다면 두 원자도 얽힘상태에 있다.

두 개의 큐비트는 4개의 기본양자상태 {|00}≡|0}|0}, |01},|10},|11}}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 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, 앞에서 살펴본 식(3)의 표현은 얽힌 상태로서, 첫번째 큐비트를 측

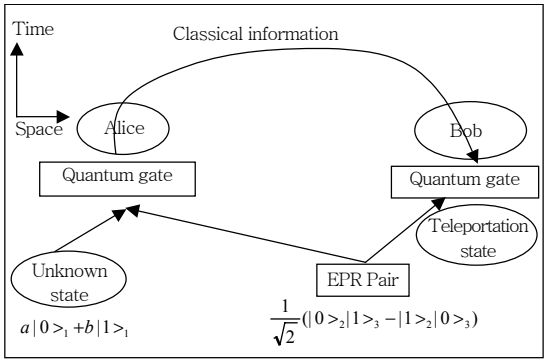
정하면 |0〉 또는 |1〉 로 될 확률이 각각 50%인데, 그 각각의 경우 두번째 큐비트는 100%의 확률로 |1〉 과 |0〉 으로 된다. 멀리 떨어져 있는 두 큐비트가 얽혀 있을 때, 한 큐비트의 측정이 다른 큐비트에 영향을 미치므로 양자 역학의 비국소성(non-locality)을 보여준다.

얽힘편광상태에 있는 두 광자는 어떠한 편광상태에도 있을 수 있는 모든 가능성을 가지고 있고, 단지 두 광자의 상대적 편광상태가 특정한 상관관계를 갖고 있다는 것 밖에는 확실히 얘기할 수 없다. 그러나 일단 측정이 수행되면 측정방법과 측정결과에 따라 양자 상태함수의 붕괴를 통해 두 광자의 편광상태가 확정된다. 얽힘상태에 있는 두 광자의 이러한 특성은 양자원격이동의 기본이 된다.

2. 양자원격이동

일반적으로 원격이동이라 하면, 공상과학영화에서 나오던 물체의 위치이동을 생각하지만, 양자원격이동은 물체가 실제로 움직이는 것이 아니라 입자가 공간상에 떨어진 다른 입자로 전이되는 현상을 말한다.

No-cloning 이론에 의하면 알려지지 않은 상태벡터를 원본으로 유지하면서 복사하는 유니터리 변환은 없다. 그러나 알려지지 않은 상태벡터의 원본을 파괴하면서 공간적으로 떨어진 지점에서 원본과 같은 상태벡터를 가진 양자계를 만들어 내는 것은 가능하며 이를 양자원격이동이라 한다((그림 5) 참조).



(그림 5) 양자원격이동

양자원격전송의 의의는 깨지기 쉬운 양자정보를 손실 없이 전달할 수 있는 방법을 제공한다는 데 있다. 양자정보를 전달하는 상황을 고려할 때, 원자를 직접 운반할 경우 양자상태가 이미 붕괴했을 거리를 양자원격전송은 손실 없이 정보를 전송할 수 있다.

또한, 서로 다른 종류의 양자계 사이의 양자정보 교환을 매개하는 원리로 사용될 수 있다. 예를 들어 양자컴퓨터 사이에 큐빗을 교환하려 할 때 원자를 직접 교환하는 것보다 광섬유를 통해 광자를 보내는 것이 낫다. 이때 양자원격전송은 광자와 큐빗을 저장하는 원자 혹은 기타 양자계 사이의 손실 없는 양자정보의 교환을 가능하게 해 줄 것이다.

V. 결 론

Shor의 소인수분해 알고리듬은 소인수분해 문제나 이산로그 문제의 복잡 난해함에 근거를 두고 있는 공개키 암호 체계에 큰 영향을 미칠 수 있고[12], [13], Grover의 검색 알고리듬은 DES와 같은 비밀키 암호 체계에 위협을 가할 수 있어, 양자 알고리듬의 개발은 앞으로의 미래 사회에 매우 큰 영향을 미칠 수 있다[14].

현재 우리나라 나노기술은 선진국과 상당한 기술격차를 나타내고 있으며, 선진국과 같은 대규모의 지원과 투자를 기대할 수 없는 상황에서 한정된 자원으로 많은 성과를 이루어야 한다.

따라서, 국제 협력이나 해외연구기관과의 교류를 통해 선진 기술을 경험하고 정보를 습득하는 것이 중요하다. 이를 위해서는 선진 나노기술 정보의 습득과 체계화된 DB 구축으로 나노기술 정보 선진화를 이루는 것이 필수적이다.

양자정보통신의 각 분야기술이 아직은 기초연구 수준에 있지만 세계적으로 그 중요성을 인식하고 대규모 투자를 아끼지 않는 분야이기 때문에, 차후에 이 분야의 개발을 시작하면 기술 종속 또는 이 분야 기술에 대한 후진국으로 전락할 수가 있다. 그러므로, 외국의 기술 발전 추세에 대처할 수 있는 기반 기술을 확보하는 연구를 지속적으로 수행할 필요가 있다.

참 고 문 헌

[1] G.E. Moore, *Electronics*, Vol. 38, No. 7, 1965, p. 114 .

[2] R.W. Keyes. *IBM. J. Res. Dev. 32,* Vol. 24, 1988, p. 24.

[3] D.J. Griffiths, *Introduction to Quantum Mechanics*, Prentice-Hall, 1994.

[4] D.P. Chi and J. Kim, Quantum database search by a single query, *Proceedings of First NASA International Conference on Quantum Computing and Quantum Communication*, Palm Springs, CA, Lecture Notes in Computer Science, Springer-Verlag, Vol. 1509, 1999, pp. 148 - 151; Chaos, Solitons and Fractals, Vol. 10, 1999, pp. 1689 - 1693.

[5] C.H. Bennet and G. Brassard, *Proc. IEEE Int. Conference on Computers, Systems and Signal Processing, IEEE*, New York, 1984.

[6] C.H. Bennet, "Quantum Information and Compuation," *Phys. Today*, Vol. 48, No. 10, Oct. 1995, pp. 24 - 30.

[7] P.G. Kwiat et al., "New High Intensity Source of Polarization-Entangled Photon Pairs," *Phys. Rev. Lett. 751995*, pp. 4337 - 4341.

[8] S. Wieder, *The Foundations of Quantum Theory,* Academic Press, 1973.

[9] E. Hagley et al., "Generation of Einstein-Podolsky-Rosen Pairs of Atoms," *Phys. Rev. Lett. 79*, 1997. pp. 1 - 5.

[10] M.A. Nielsen and I.L. Chuang, *Quantum Computation and Quantum Information*, Cambridge, Cambridge University Press, 2000.

[11] A. Zeilinger, Scientific American, April 2000, p. 32; The Physics of Quantum Information, edited by D. Bouwmeester, A. Ekert, and A. Zeilinger, Springer-Verlag, Berlin, Ch. 3, 2000.

[12] P.W. Shor, *Proceedings 35th Annual Symposium on Foundations of computer Science*, IEEE Computer Society Press, Los Alamitos, CA, 1994, p. 124.

[13] P. Shor, in *Proc. of 35th Annual Symposium on the Foundations of Computer Science*, IEEE Computer Society, Los Alamitos, p. 124(Extended Abstract) 1994, *SIAM Journal on Computing 26*, 1997, p. 1484.

[14] L.K. Grover, "A Fast Quantum Mechanical Algorithm for Database Search," *Proceedings of the 28th Annual ACM Symposium on Theory of Computing,* New York, ACM, 1996, pp. 212 - 219; *Physical Review Letters*, Vol. 79, 1997, pp. 325 - 328.