광자 기반 양자연산

최상경
한국표준과학연구원

요 약

한국표준과학연구원 (Korea Institute of Standards & Science, KRISS)에서 수년간 수행한 연구를 중심으로 단일광자 기반 양자연산에 대해서 알아본다. 자발매개하향변환에 의한 광자쌍 발생에서 생성된 얽힘으루부터 복잡한 얽힘구조를 만들고 이용해서 양자연산까지 실행하는 과정을 살펴본다.

Ⅰ. 서 론

양자정보란 양자비트 또는 큐비트 (qubit)로 인코딩 (encoding)한 정보를 말한다. 디지털 비트는 "0"과 "1"로 명명된 두 가지 상태만 가능하지만, 큐비트는 디락표기 (Dirac notation)으로 나타낸 $|0\rangle$ 상태와 $|1\rangle$ 상태뿐만 아니라 그 두 양자상태 간의 중첩도 가능하다. 여기서, 디지털의 경우든 양자의 경우든, "0"과 "1"은 서로 구별되는 라벨로 쓰여진 것이고, $|0\rangle$과 $|1\rangle$은 서로 구별되는 양자상태를 가리킨다. $|0\rangle$과 $|1\rangle$만으로 존재하는 큐비트는 디지털비트와 다를 바가 없지만, 중첩된 양자상태로 존재하는 큐비트는 복제가 원리적으로 불가능하고, 결잃음 (decoherence)의 영향을 받으면 쉽게 깨진다. 이러한 특성을 가진 양자정보는 디지털 정보시스템으로 구현이 불가능한 알고리듬 또는 프로토콜을 실행할 수 있는 잠재성을 지니고 있다. 예를 들면, 도청을 몰래 할 수 없는 양자암호 프로토콜이 가능하다. 또한, 검색 및 소인수분해와 같이 시간이 많이 소요되는 작업을 디지털연산에 비해 원리상 초고속으로 처리하는 양자연산 알고리듬이 가능하다. 디지털 정보처리와 확연히 구별되는 양자정보처리가 이론적으로 가능한 이유는 양자정보가 고전물리의 범주를 벗어난 양자물리의 특성을 적절히 활용하기 때문인데, 실제로 구현가능한지는 별개의 문제이며 실험자들에게 큰 도전이다.

논의를 더 진행하기 전에 양자연산 및 양자컴퓨터를 정의할 필요가 있다. 우리가 흔히 사용하는 디지털컴퓨터도 미시적으로 관측하면 양자물리의 법칙을 따라 동작하지만 양자연산 장치는 아니다. 우리가 말하는 양자연산은 디지털 논리로 원론적으로 실행이 안되는 양자변환을 이용한 알고리듬에 따라 계산하는 것을 의미한다. 디지털연산을 초월하는 양자연산의 비고전적 성능은 양자정보의 중첩이 가능하다는 점, 특히 얽힘이 가능하다는 점과 밀접한 관련이 있다[1]. 얽힘은 양자물리의 전제들로부터 필연적으로 나타나는 이론적인 구조물이다. 물리계가 얽힘상태 (entangled state)에 존재하면, 그 파동함수는 물리계를 구성하는 부분물리계들의 파동함수의 곱으로 나타낼 수 없다. 이러한 얽힘상태는 1980년대부터 수많은 사람들이 실험적으로 관측하였고, 벨 부등식 (Bell's inequality)를 위배하는 현상이 그 실험의 내용이다. 고전물리에서 전제한 국소현실주의 (local realism)의 경계에 해당하는 벨 부등식을 넘어서는 얽힘상태의 존재로부터 현실세계는 근본적으로 확률적이거나 비국소적 결정론 (nonlocal determinism)을 따른다는 기묘한 결론이 나온다.

양자연산을 구현하는 플랫폼은 큐비트 구현 및 큐비트 간의 양자상호작용이 가능한 물리계의 종류만큼 다양하다: 빛, 원자, 이온, 핵스핀 액체, 양자점, 초전도 고리 등 여러 가지가 제안되

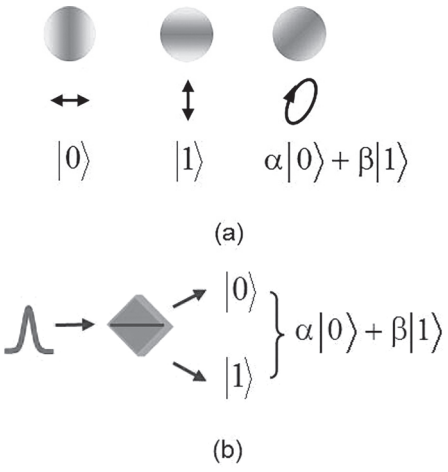

그림 1. (a) 단일광자의 수직편광상태 $|0\rangle$ 및 수평편광상태 $|1\rangle$의 중첩이 가능한 편광큐비트 (b) 단일광자 펄스가 분할기를 지난 후 윗경로상태 $|0\rangle$ 및 아랫경로상태 $|1\rangle$의 중첩이 가능한 경로큐비트.

었다. 이 중에서 중첩이 가능한 빛의 성질에 큐비트를 표기하는 선형광학 (linear optics) 방식이 잠재성이 높고 기술적으로 구현이 용이하다[2]. 이 방식은 단일광자 (single photon)으로 구성된 빛펄스 (이하 '광자')를 큐비트 매개체로 사용하고, 광자의 성질에 인코딩한 광큐비트 (photonic qubit)가 양자정보의 단위이다. 중첩이 가능한 어떠한 광자의 성질도 큐비트 인코딩에 활용할 수 있는데, 편광, 경로, 주파수, 시각 (time-bin), 공간모드 등이 실험적으로 구현된 바가 있다. 가장 대표적으로 사용하는 광큐비트는 편광큐비트이고, 경로큐비트도 보조로 사용한다 (〈그림 1〉 참조).

선형광학 방식의 양자연산은 광큐비트들이 생성되는 초기단계와 연산결과가 측정되는 최종단계 사이의 광시스템에서 광큐비트의 양자상태에 대해 선형 유니터리변환을 작용한다. 선형광학 방식의 장점은 크게 두 가지이다: 첫째, 재고주문형 (off-the-shelf) 광부품을 구하기 쉽게 때문에 프로토타입 시스템 구축이 용이하다; 둘째, 자유공간에서 이동하는 광자의 양자상태는 결잃음을 당할 가능성이 없다. 그러므로 광큐비트의 얽힘상태는 외부환경의 잡음이나 충격에 의해 깨질 염려가 없다.

선형광학 방식의 단점도 여러 가지 있다. 광큐비트들 사이의 상호작용이 자유공간에서 일어나지 않으므로, 한 큐비트의 값에 따라 다른 큐비트의 값이 변하려면 그 사이에 비선형 매질 또는 장치의 작용이 필요하다는 점이 선형광학 방식을 제약한다. 또한, 광속으로 이동하는 광자를 잠시 멈추게 하거나 그 양자상태를 메모리에 일시보관하기 쉽지 않다. 단일광자 광원의 생성효율이나 단일광자 검출기의 검출효율이 지속적으로 향상되었지만 실용화까지는 기술적인 어려움들이 상당하다. 그러나, 무엇보다도 가장 근원적인 한계는 선형광학 방식의 양자연산 실행의 성공이 확률적이라는 점이다. 광자쌍 생성이 저조한 확률로 일어나고, 연산의 난이도가 높을수록 필요한 큐비트는 많아지고 선형광부품은 많아지면서 성공한 연산에 해당하는 최종결과가 검출될 확률은 급속히 작아진다.

근본적인 한계에도 불구하고 선형광학 방식이 연구의 대상이 되는 것은, 프로토타입 양자연산 시스템을 상대적으로 용이하게 구현할 수 있고, 그 양자연산의 실행은 멀티큐비트 얽힘의 생성과 직결하고 단일광자 제어수준을 반영하기 때문이다. 선형광학 방식으로 실행한 양자연산은 광큐비트 얽힘상태 중에서도 클러스터 상태 (cluster state)가 필요하다. 클러스터 상태 (일명 그래프 상태, graph state)는 클러스터 (혹은 그래프)로 표현할 있는 얽힘상태를 말하는데, 각 꼭지점은 큐비트에 해당하고, 그 사이의 연결선은 제어된 Z (controlled Z) 게이트로 연결된 얽힘관계를 나타낸다.

이러한 클러스터 상태를 양자연산 시스템으로 활용할 수 있

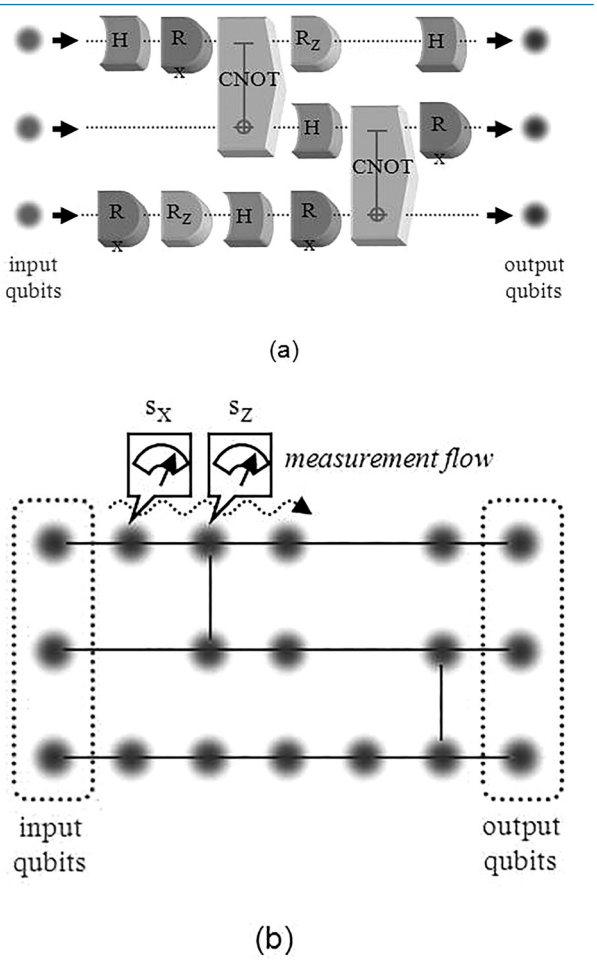

그림 2. (a) 양자논리회로 (b) 클러스터 상태 [4].

다. 그 이유는, 양자연산회로의 구조와 클러스터 상태의 구조 사이에는 일대일 관계가 성립하기 때문이다. 그러므로, 그림 2(a)의 도식처럼 n개의 양자게이트가 필요한 양자연산을 실행하기 위해서는 그 양자회로의 구조에 대응하는 클러스터 상태를 만든 뒤, 각 큐비트의 상태를 차례대로 일정한 규칙에 따라 측정하면 된다[3]. 즉, 〈그림 2(b)〉의 가장 왼쪽 열부터 시작해서 한 열의 큐비트들을 측정한 결과에 따라 다음 열의 큐비트들에 대한 측정방식을 조정한 후에 측정하는 과정을 반복해서 얻은 가장 오른쪽 열을 이루는 큐비트들의 측정결과가 곧 연산결과이다. 이러한 양자연산 과정은 클러스터상태를 이루는 큐비트들의 얽힘관계가 순차적으로 끊어지는 비가역과정이다. 그래서 선형광학 방식의 양자연산을 단방향양자연산 (one-way quantum computation, 1WQC)이라고도 부른다.

KRISS에서 단일광자 기반 측정기술 확립을 목표로 삼아서 단일광자의 양자상태 생성, 제어, 측정에 관한 기술을 개발하고 있다[4]. 그 일환으로 선형광학 방식의 양자연산을 구현하기 위한 연구를 수행하였고, 그 과정을 요약하면 다음과 같다:

우선 비선형 광매질에서 자발매개하향변환 (spontaneous parametric down-conversion, SPDC)을 일으켜서 편광얽힘 광자쌍을 생성한다. 광큐비트 개수를 증가시키기 위해 광자쌍 개수도 늘리고, 분할기를 이용해서 이미 편광큐비트를 갖춘 각 광자에 경로큐비트도 인코딩한다. 이처럼 2개의 큐비트가 인코딩된 광자들을 얽혀서 선형 클러스터 상태를 생성한다[5]. 더 나아가 분할기 및 검출기를 이용한 융합게이트를 구현해서 서로 독립적인 선형 클러스터 상태들이 얽히게 만든다. 그 결과로 더욱 많은 광큐비트들이 진정한 얽힘 (genuine entanglement)을 이룬 클러스터 상태를 생성하고, 이것을 활용한 단방향양자연산으로 기초적인 양자알고리듬을 실행한다[6]. 양자연산의 성공적인 실행은 단일광자 양자상태를 다루는 기술의 수준을 검증하는 척도로 활용한다.

본론에서는 SPDC 광자쌍 발생에 의한 얽힘 생성 부터 선형광학 방식의 양자연산까지의 과정을 설명한다: 참고문헌 [4]를 인용해서 SPDC 광자쌍 발생에 의한 얽힘 생성을 설명하고, 참고문헌 [6]을 인용해서 광큐비트 간의 얽힘으로부터 양자연산까지 실행하는 과정을 설명한다. 결론에서 현재의 이슈를 바탕으로 미래에 관한 단상을 서술한다.

Ⅱ. 본 론

광자쌍을 생성하는 SPDC라는 비선형 효과의 동작원리는 〈그림 3〉과 같다.

유전체 매질의 편광이 외부에서 가해진 전기장에 비례한다는 선형어림은 대체로 유효하지만, 전기장의 세기가 매우 강하면 편광에 대한 전기장의 비선형 고차항을 무시할 수 없다. 비선형 매질에 충분히 강한 전기장을 가하면 매질에서 생기는 편광은 전기장의 제곱 또는 그 이상에 비례할 수 있다. 예를 들면, 전기장의 제곱항을 고려해야 하는 소위 $\chi^{(2)}$ 결정체에 펌프광이라 불리우는 강한 레이저광이 입사해서 매질 안의 위상정합 (phase matching) 조건을 만족하면, 진공요동의 자극을 받은 무작위의 펌프광자가 두 개의 광자로 쪼개지는 현상이 일어날 수 있다. 매우 작은 확률로 일어나는 이 비선형 광현상을 SPDC라고 부른다[7].

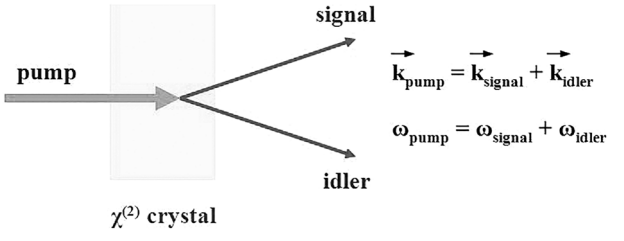

그림 3. χ(2) 매질에서의 자발매개하향변환에 의해 펌프 (pump) 광자는 신호 (signal) 광자와 여분 (idler) 광자로 나뉘고, 세 광자 사이에 에너지 및 운동량 보존 법칙이 성립함. 생성된 두 광자 중 주파수가 큰 것을 통상 신호 광자라고 부름 [4].

우리는 베타-붕화바륨 (β-barium borate, BBO)라는 비선형 결정체 매질에서 SPDC를 통해서 광자쌍 을 확률적으로 생성한다. 결정체는 SPDC 전후로 변화가 없으므로 에너지 및 운동량 보존 법칙은 광자들에게만 적용되고, 〈그림 3〉처럼 광자쌍 생성과정 전후의 광자들의 주파수 및 운동방향 사이에 각각 상관관계가 성립한다. 우리는 SPDC로부터 발생한 두 광자의 선편광 (linear polarization)이 같은 방향인 위상정합 조건에서 실험한다. 광정렬이 비교적 간편하고, 생성되는 광자쌍의 선폭이 상대적으로 넓어서 생성률이 더 높아지는 기술적인 장점 때문이다.

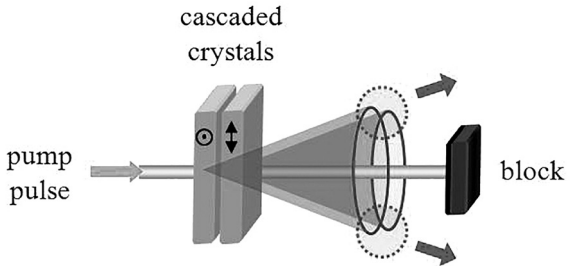

그림 4. 계단식 비선형 결정체의 SPDC에 의한 광자쌍 편광얽힘 생성. 붉은 원은 광자를 나타냄 [4].

그러나, 각기 다른 방향으로 운동하는 두 광자의 편광은 아직 서로 얽히지 않았다. 광자쌍을 구성하는 광자 간의 편광얽힘을 생성하려면 비구별성 (indistinguishability)를 부여해야 하는데, 〈그림 4〉처럼 비선형 결정체 2개를 사용하는 방법이 있다. 두 개의 동일한 비선형 결정체를 계단식 (cascade) 형태로 붙이는데, 두 결정체의 광축이 서로 수직이 되도록 접합하고, 입사하는 펌프광의 편광방향이 45° 가 되도록 한다. 그렇게 하면, SPDC에 의해 광자쌍이 앞쪽 결정체에서 발생하면 두 광자는 수평편광상태를 갖게 되고, 뒤쪽 결정체에서 발생하면 두 광자는 수직편광상태를 가진다. 여기서 펌프광 펄스의 결맞음길이에 비해 결정체들의 두께가 충분히 작고, 결정체내 두 편광성분 간의 군속도 차이에 기인한 비껴나감 (walkoff)를 적절한 복굴절 매질을 추가해서 보상하면, 광자쌍의 편광상태를 생성한 결정체가 어느 것인지를 측정 이전에 알 수 있는 방법은 원천적으로 없다. 즉, 수평편광 H와 수직편광 V의 가능성들이 간섭해서 서로 얽혔고, 그 얽힘상태 $|\psi\rangle$를 수식으로 표현하면 다음과 같다:

$$|\psi\rangle = (|HH\rangle + |VV\rangle)/\ 2^{1/2}$$

참고로, 위의 $|\psi\rangle$는 가장 간단한 2-큐비트 얽힘상태인 벨상태 (Bell state) 중의 하나를 나타낸 것이며, 2개의 큐비트가 서로 얽힌 상태를 도식적으로 ●—● 로 나타낸다.

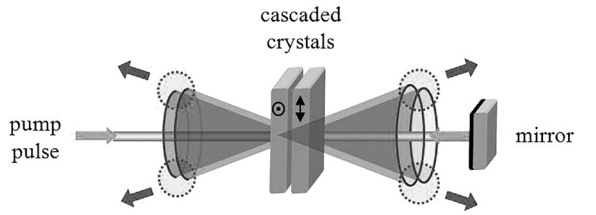

그림 5. 펌프광이 거울에 반사되고 SPDC 매질을 이중통과하여 생성한 각 광자쌍마다 편광얽힘 생성 [4]. 두 광자쌍의 얽힘상태들은 서로 얽히지 않았음.

SPDC를 선형광학계의 얽힘광원으로 유용하게 사용하지만 여러 기술적인 제약들이 따른다. 우선, SPDC에 의한 광자쌍 발생은 시간상 무작위로 일어나기 때문에 주문식 (on-demand) 생성이 곤란하다. 광자쌍은 또한 〈그림 4〉가 묘사한 생성원뿔 중심축을 기준으로 서로 반대편에 발생하는데, 원뿔의 둘레를 따라 무작위로 발생한다. 이 상황에서 정확히 1개의 광자쌍 발생을 최대한 보장하려면 2개 이상의 광자쌍이 동시발생할 가능성을 극소화해야 한다. 펌프광의 세기를 충분히 줄이면 복수 광자쌍 발생 문제가 거의 해결되지만, 대신에 광자쌍 생성률이 저하된다. 이러한 접근방식은 주문식 단일광자 광원 개발에 쓰인다.

그러나, 서로 얽힌 광큐비트 개수를 증가시키려면 서로 구별되는 복수의 광자쌍이 동시에 발생할 확률을 최대한 높이는 방법이 적당하다. 〈그림 5〉는 계단식 결정체에서 거울 반사에 의한 펌프광 이중통과를 이용해서 2개의 얽힘광자쌍을 동시발생시키는 방법인데, 그 생성 확률은 1개의 광자쌍 생성하는 것에 비해 제곱배 낮다. 광자쌍 생성률을 높이기 위해 펌프광의 세기를 지나치게 높이면 결정체가 손상되므로, 지금까지 알려진 비선형 결정체 재료를 사용해서 3개의 광자쌍 동시발생시키는 것이 현재기술의 최고수준으로 보인다.

광큐비트 개수를 늘리는 방법은 광자쌍 개수 증가 외에 각 광자에 복수의 큐비트를 인코딩하는 것이다. 흔히 사용되는 이중인코딩 방식은 편광큐비트이 이미 갖춰진 광자에 대한 경로큐비트의 추가인코딩인데, 우리는 두 가지 방법을 사용한다.

첫째 방법은 편광큐비트를 갖춘 광자가 편광분할기 (polarizing beamsplitter, PBS)의 작용을 받는 것이다. 〈그림 6(a)〉에 나와 있듯이, 편광이 수평 또는 수직이냐에 따라 광자가 통과 또는 반사되도록 작용하는 PBS는 광자에게 통과경로 $|0\rangle_s$와 반사경로 $|1\rangle_s$가 기반이 되는 경로큐비트를 부여한다.

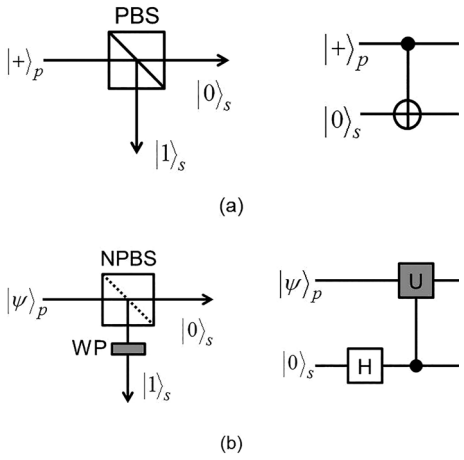

그림 6. (a) 편광분할기 (PBS)를 이용한 경로큐비트 인코딩
(b) 비편광분할기 (NPBS)를 이용한 경로큐비트 인코딩.
$|+\rangle$: 수평편광 $|0\rangle_p$ 및 수직편광 $|1\rangle_p$의 중첩상태, p: 편광큐비트, s: 경로큐비트. (a), (b)의 각 우측에 양자회로도를 나타냄.

양자회로도 (quantum wire diagram)으로 표현하면, 제어큐비트인 편광큐비트와 표적큐비트인 경로큐비트로 구성된 제어된 NOT (controlled NOT) 작용에 해당한다.

둘째 방법은 편광큐비트를 갖춘 광자가 비편광분할기 (nonpolarizing beamsplitter, NPBS)의 작용을 받는 것이다. 〈그림 6(b)〉를 보면, 입사하는 광자는 통과경로 $|0\rangle_s$ 및 반사경로 $|1\rangle_s$로 표현되는 경로큐비트를 갖게 된다. 반사경로에 놓인 파장판 (waveplate, WP)는 임의의 유니터리 변환U의 역할을

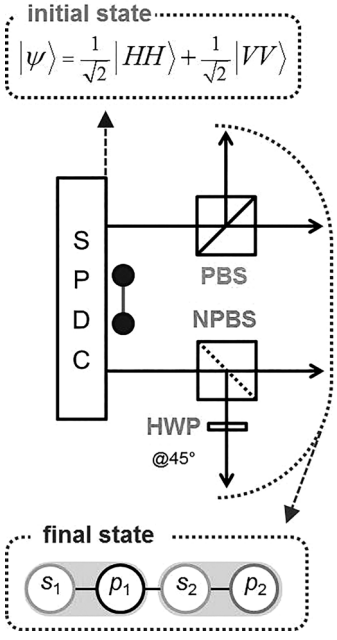

그림 7. 편광큐비트이 인코딩된 얽힘광자쌍의 각 광자에 경로큐비트를 추가로 인코딩해서 2-광자 4-큐비트 선형 클러스터상태를 생성함. p: 편광큐비트, s: 경로큐비트, 1: 광자 1, 2: 광자 2.

수행한다. 이 방법에 대응하는 양자회로도를 보면, 하다마드게이트 (Hadamard gate)의 작용을 받아서 중첩상태가 된 경로큐비트가 제어큐비트이고 편광큐비트가 표적큐비트인 제어된 유니터리 (controlled unitary) 작용이다.

편광얽힘상태를 이루는 광자쌍에 두 가지 경로큐비트 추가인코딩 방법을 적용하면 2-광자 4-큐비트 선형 클러스터 상태를 만들 수 있는데[5], 그 방법을 〈그림 7〉이 도식적으로 나타내고 있다. SPDC 광자쌍은 초기에 수평편광 및 수직편광이 얽힌 상태에 있다. 편광큐비트를 갖춘 각 광자에 경로큐비트를 추가하는데, 한 광자에 PBS 인코딩 방식을 적용하고, 다른 광자에 반파장판 (half-wave plate, HWP)를 사용한NPBS 인코딩 방식을 가한다. 각 광자에 경로큐비트를 서로 다른 방식으로 인코딩하고 45° 에 맞춘 HWP를 사용한 이유는 결과적으로 편광큐비트 및 경로큐비트 모두가 선형으로 얽힌 클러스터상태를 만들기 위해서이다. 〈그림 7〉의 보라색 점선에 도달한 광자쌍의 2개의 편광큐비트 및 2개의 경로큐비트는 선형으로 얽힌 2-광자 4-큐비트 (2-photon 4-qubit, 2P4Q) 클러스터 상태를 구성하고 있다.

앞에서 본 〈그림 5〉처럼 계단식 결정체를 이중통과한 펌프광을 이용해서 생성한 2개의 광자쌍에 〈그림 7〉의 복수인코딩 방식을 적용하면, 서로 독립적인 2P4Q 선형 클러스터상태 2개를 얻을 수 있다. 더욱 복잡한 구조의 클러스터상태를 만들려면 서로 독립적인 클러스터들을 얽혀서 합쳐야하는데, 그 얽힘융합을 실행하는 것이 융합게이트 (fusion gate, FG)이다.

〈그림 8〉은 서로 다른 광자에 인코딩된 경로큐비트를 합치는 융합게이트를 나타낸 것이다. 융합은 단일광자계수기 (single-photon counter, SPC)들이 동시계수하는 경우에만 일어난다. 이 때, 광자 1의 경로큐비트 및 광자 2의 경로큐비트가 융합되어서 광자 1의 경로상태 $|0\rangle_1$ 및 광자 2의 경로상태 $|1\rangle_2$는 각각 융합된 경로큐비트의 $|0\rangle$ 및 $|1\rangle$로 변환한다. 수식으로 표현하면, 융합게이트는 $|0\rangle\langle 00|_{12} + |1\rangle\langle 11|_{12}$투사 (projection)에 해당한다. 이러한 융합게이트를 2개의 2P4Q 클러스터상태

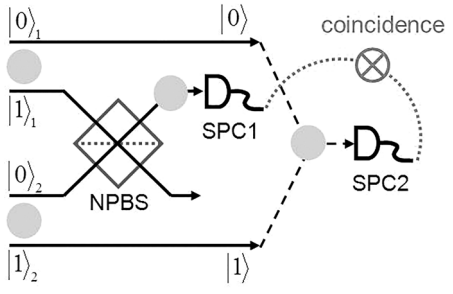

그림 8. NPBS를 이용한 경로큐비트 융합게이트. 계수기 SPC1 및 SPC2가 동시계수하는 경우에만 융합이 일어남. 아래첨자 1, 2는 광자 1, 광자 2를 나타냄.

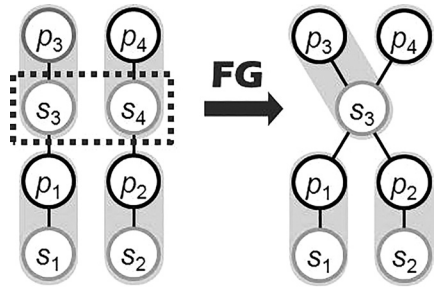

그림 9. 융합게이트는 각 2P4Q 클러스터 상태의 경로큐비트를 융합해서 4P7Q 클러스터 상태를 생성함 [6].

에 가하면 4개의 광자에 인코딩된 7개의 큐비트가 서로 얽힌 4P7Q 클러스터상태를 얻을 수 있다. 〈그림 9〉가 융합의 작용을 도식으로 나타냈는데, 융합으로 인해서 7개의 큐비트들이 모두 서로 얽힌 진정한 얽힘을 이룬 것이 주목할 점이다.

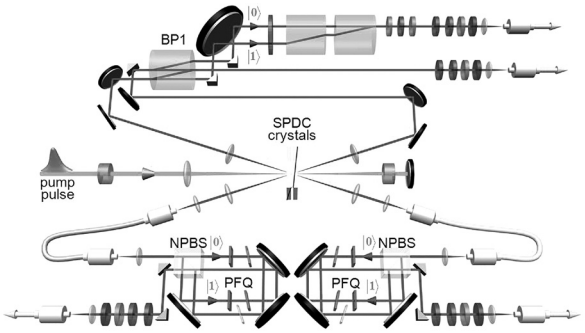

그림 10. 4-광자 7-큐비트 클러스터 얽힘상태를 생성하고 측정하는 실험구도 [6].

지금까지 소개한 SPDC 광자쌍 생성, 광자당 복수인코딩, 융합게이트 등의 구성요소들을 모두 조합한 실험구도를 나타낸 것이 〈그림 10〉이다. 실험의 안정도를 높이기 위해 사용한 사냑 간섭계 구도를 사용하는데, 여기서 편광뒤집기 결정체 (polarization flip quartz, PFQ)의 역할은 〈그림 7〉의 HWP와 같다. 역시 실험안정도 향상을 위해 2P4Q 클러스터 생성에 필요한 PBS의 역할 및 융합게이트의 역할을 복굴절 프리즘 (birefringent prism, BP)인 BP1이 한꺼번에 수행한다.

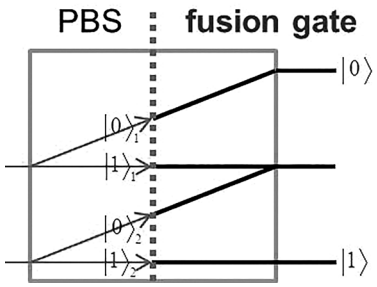

그림 11. 복굴절 결정체 BP1의 앞부분은 편광분할기, 뒷부분은 융합게이트 역할을 수행함 [6].

〈그림 10〉의 실험구도에 나온 BP1을 더 자세히 묘사한 것이 〈그림 11〉이다. BP1의 앞부분은 경로큐비트 추가인코딩을 위한 그림 7의PBS를 대신한 것이고, BP1의 뒷부분은 〈그림 8〉의 융합게이트처럼 서로 다른 광자의 경로를 합치는 역할을 수행한다.

이렇게 생성한 4P7Q 클러스터상태를 2-비트 함수에 대한 도이치-요차 알고리듬 (Deutsch-Josza algorithm, DJA) 실행에 적용할 수 있다. 2-비트 함수란 입력값의 크기가 2비트이고 출력값의 크기가 1 비트인 함수를 말한다. 이 중에서 상수함수는 입력에 상관없이 출력이 상수인 함수이고, 균형함수는 출력값이 0인 경우와 1인 경우의 개수가 동일한 함수이다. 그림 12의 진위표에서 (i)과 (ii)는 f(x)가 상수함수인 경우들이고, (iii)~(viii)는 f(x)가 균형함수인 경우들이다.

$f(x)$	(i)	(ii)	(iii)	(iv)	(v)	(vi)	(vii)	(viii)
$f(00)$	0	1	0	1	0	1	0	1
$f(01)$	0	1	0	1	1	0	1	0
$f(10)$	0	1	1	0	0	1	1	0
$f(11)$	0	1	1	0	1	0	0	1

그림 12. 2-비트 함수 중에서 상수함수 (i), (ii) 및 균형함수 (iii)~(viii)의 진위표.

2-비트 함수가 상수함수 및 균형함수로 국한된 경우, 주어진 함수 f(x)가 〈그림 12〉의 어느 경우에 해당하는지를 최소한의 측정횟수로 알려면 어떻게 해야 하는가? 고전적인 디지털알고리듬으로 알아내려면 f(x)를 최소한 2회, 대개는 3회 측정해야 f(x)가 상수함수인지, 균형함수인지 알 수 있다.

양자알고리듬을 실행하면 1회 측정으로 f(x)가 상수함수인지 균형함수인지 알 수 있다. 그러나, 우리가 4P7Q 클러스터상태를 활용해서 실행하려는 양자연산은 미지의 2-비트 함수에 대

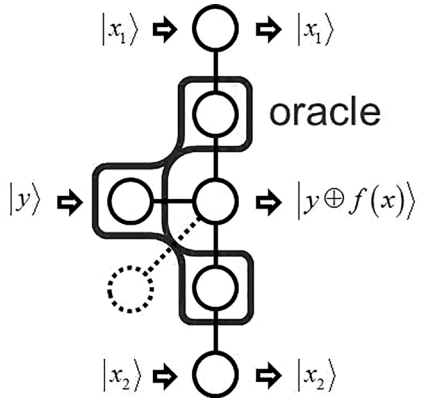

그림 13. 4P7Q 클러스터 상태를 이용한 2-비트 도이치-요차 알고리듬 연산. |x1⟩, |x2⟩: 입력큐비트, |y⟩: 보조큐비트.

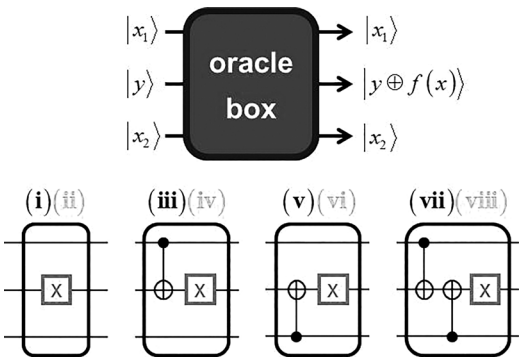

그림 14. 함수의 진위표 대칭성에 따라 오라클의 연산이 달라짐.

한 DJA가 아니라, 이미 알고 있는2-비트 함수에 대해 DJA 연산이 제대로 실행되는지를 확인하는 것이다.

4P7Q 클러스터상태를 활용하면 〈그림 13〉처럼 큐비트2개는 입력큐비트, 1개는 보조큐비트, 3개는 오라클 (oracle)로 사용하고, 여분 1개는 필요가 없다. 참고문헌 [8]의 프로토콜을 따르면, 오라클을 1회 연산시킨 후에 그 결과를 측정하면, f(x)가 상수함수인지 균형함수인지를 알 수 있다. 그러나, 우리가 실행하는 DJA 연산은 주어진 2-비트 함수 f(x)의 진위표 대칭성에 따라 오라클을 실행한 측정결과가 예상대로 나오는지 확인하는 것이다.

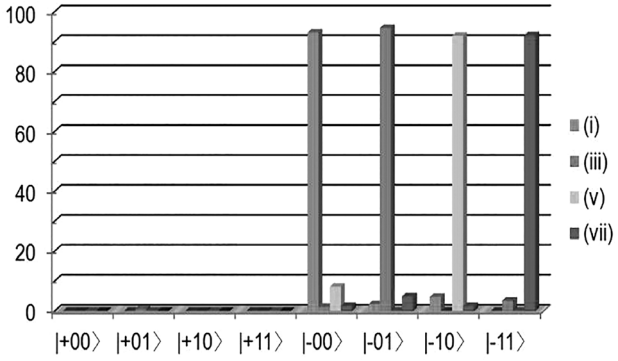

그림 15. 2-비트 도이치-요차 알고리듬 실행 후 |y x1 x2⟩ 의 각 측정결과가 각 함수에 대해 나타나는 확률.

〈그림 14〉에 양자회로도로 나타낸 것처럼 오라클은 함수 (i), (iii), (v), (vii)에 대해 각기 다른 연산을 실행한다. 그래서, 3-비트 입력상태 $|y\ x_1\ x_2\rangle$ 에 대한 DJA 연산결과는 네 가지 함수마다 다르게 나타난다. 성공한 연산은 그 특성상 $|y\rangle = |-\rangle$ 중첩상태인 경우에 국한되고 $|y\ x_1\ x_2\rangle$ 가 가질 수 있는 네 가지 값들이 DJA 연산결과로 나타나는 함수별 확률들은 〈그림 15〉와 같다. 오라클이 이미 '알고' 있는 함수에 맞는 연산결과가 나올 확률은 어느 경우든 90%를 상회한다.

Ⅲ. 결 론

KRISS에서 수행한 선형광학 방식의 양자연산을 구현하려는 연구내용을 살펴보았다. 단일광자 생성 및 얽힘에서 시작해서 기초적인 양자연산 실행까지 달성하였다. 그러나, 서론에서 언급한 여러 가지 제약 때문에 단일광자 기반 선형광학 방식이 현재 기술수준에 기인한 한계에 부딪치고 있어서 양자연산 구현을 위한 구성요소의 성능향상이 필요하다. 주문식 단일광자 광원, 광자수 분해능 검출기, 나노공정 광회로 등의 개발이 성과를 보이면 이론에 불과한 모델의 실제구현도 가능하다. 현재는 10개 내외의 광큐비트 얽힘이 한계이어서 실현할 수 있는 프로토타입 범위는 제한적이지만, 제어가능한 광큐비트 개수가 20개 수준이 되면 양자시뮬레이션 등 양자정보를 응용하는 새로운 시도가 가능할 것으로 보인다. 그리고, 단일광자 생성 및 측정에 관한 요소기술 향상이 양자정보통신의 실용화 및 양자현상을 이용한 측정기술의 확립에 기여할 것으로 기대한다.

참 고 문 헌

[1] C. H. Bennett and D. P. DiVincenzo, Nature 404, 247 (2000).

[2] P. Kok, W. J. Munro, K. Nemoto, T. C. Ralph, J. P. Dowling, G. J. Milburn, Rev. Mod. Phys. 79, 135 (2007).

[3] R. Raussendorf and H. J. Briegel, Phys. Rev. Lett. 86, 5188 (2001).

[4] 최상경, 박희수, "물리학과 첨단기술"2010년 10월호 pp. 11-15.

[5] H. S. Park, J. Cho, J. Y. Lee, D.-H. Lee, and S.-K. Choi, Opt. Express 15, 17960 (2007).

[6] S. M. Lee, H. S. Park, J. Cho, Y. Kang, J. Y. Lee, H. Kim, D.-H. Lee, and S.-K. Choi, Opt. Express 20, 6915 (2012).

[7] R. Boyd, Nonlinear Optics, 2nd ed., (Academic Press, San Diego, 2003).

[8] M. S. Tame and M. S. Kim, Phys. Rev. A 82, 030305 (2010).

약 력

최 상 경

1989년 서울대학교 이학사
1991년 서울대학교 이학석사
1999년 Northwestern대학교 (USA) 물리학 박사
1999년~2001년 Max-Planck-Institut für Quantenoptik (Germany) postdoc
2001년~2002년 National Physical Laboratory (UK) research scientist
2003년~2003년 Northwestern대학교 visiting scientist
2003년~현재 한국표준과학연구원 연구원
관심분야: 양자광학, 원자물리학