양자 키 분배의 이론

배준우*

1. 서론

양자 이론의 초기부터 양자 이론을 통신에 응용했던 연구 결과와 양자 얽힘에 관련한 논의는 꾸준히 있었으나, 최근 10여 년은 양자 얽힘 및 양자 상태의 정보 관점에서의 이해에 관한 연구가 가장 활발한 시기였으며, 현재는 양자 정보 이론이라는 한 분야로 자리매김하게 되었다 [1~3]. 그 시작이 되었던 두 가지 사실은, 오늘날 사용하고 있는 RSA 암호 체계가 소인수 분해 문제의 계산 복잡도를 보안성의 기반으로 하고 있다는 점과, 미래에 개발될 양자 컴퓨터 (양자 이론에 기반을 둔 전산계)가 현재 사용하고 있는 컴퓨터 (전자기학에 기반을 둔 전산계, 양자와 대비해서 고전 컴퓨터라고 부르겠다)에 비해 뛰어난 전산 능력을 가질 수 있다는 점이다. 1994년 P. Shor는 양자 소인수분해 알고리즘을 통하여 양자 컴퓨터가 고전 컴퓨터에 비해서 소인수분해를 매우 빠른 시간에 할 수 있음을 보여주었고, 이로 인하여 고전 컴퓨터의 계산 복잡도에 기반을 둔 현재의 RSA 암호 체계는 언젠가는 안전하지 않을 수 있다는 사실이 암시되었다 [4]. 실제로, 오늘날 은행 혹은 대개의 다른 보안 시스템에서는 RSA 암호 체계를 사용하고 있으므로, 양자 컴퓨터가 개발될 어느 순간에는 실제로 안전하지 않을 수 있다. 양자 컴퓨터의 개발은 그렇다면 언제쯤이나 가능할까? 아직, 이에 대한 답을 알 수 없으나, 20년, 30년 혹은 100년 후에도 양자 컴퓨터가 만들어지지 않을 것이라고 쉽게 장담할 이는 없을 것이다.

한편, 보안이라는 주제는, 현재의 도청자에게 안전해야 할 뿐 아니라 미래의 새로운 기술에 대해서도 안전해야 한다는 면에서, 현재형인 동시에 미래형이기도 하다. 따라서, 계산 복잡도에 기반을 둔 보안체계 (computational security)가 아닌, 정보 이론 측면에서의 보안성 (information-theoretic security)에 대한 연구가 요구되었으며, 소위 one-time pad라고 불리는 프로토콜은 이러한 조건을 만족한다. One-time pad에서는 비밀 (secret key) 공유가 첫 과정이자 보안에서 가장 중요한 과정이다. 여기서 비밀은 암호의 두 당사자, 흔히들 이름 짓는, 앨리스(Alice)와 밥(Bob)이 나눠가진 값들이며, 그 값들의 확률 분포는 다음의 성질을 만족한다. 0과 1의 이진수를 가정했을 때, 확률 분포는

$$P_{AB}(0,0) = P_{AB}(1,1) = 1/2 , \quad (1)$$

$$P_{ABE}(a,b,e) = P_{AB}(a,b)P_E(e) \quad (2)$$

이다. 첫 번째 조건 (1)은, 앨리스(Alice)와 밥(Bob)이 가지고 있는 시스템은 0과 1 중 특정 값에 대해서 치우친 분포를 나타내지 않음을 의미하며 이로 인해 도청자 이브(Eve) (E)는 앨리스(Alice)와 밥(Bob)이 공유한 값들을 임의로 예측할 수 없게 된다. 두 번째 조건 (2)는, 앨리스(Alice)와 밥(Bob)의 시스템이 제공하는 값들이 도청자 이브(Eve)와 독립임을 나타낸다. 고전 암호에서 앨리스(Alice)와 밥(Bob)이 멀리 떨어져서 대중 대화 시스템(Public communication)만 사용한다면, 불행하게도 비밀을 나눠가질 수 없음이 알려져 있다. 이브(Eve)가 모든 통신을 다 듣게 되어서 (2)의 조건을 만족시킬 수 없기 때문이다 [5].

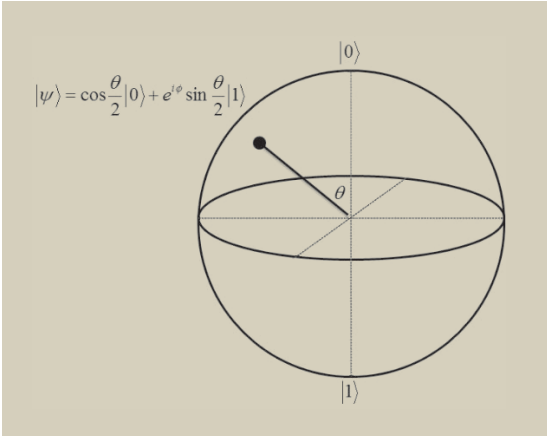
* 고등과학원

정보 이론 관점에서의 보안성 (information-theoretic security)이 요구됨으로 인해, 1984년 C. Bennett과 G. Brassard이 개발했던 양자 분배 프로토콜이, 약 15년이 지난 90년대 후반에 새롭게 인식되었다 [6]. 간략히 BB84로 불리는 이 프로토콜은 이진수 0 혹은 1을 전송하는 대신 그에 대응하는 양자 상태들을 전송하고 측정함으로써 비밀 키를 공유할 수 있도록 한다. 이러한 양자 키 분배는 원칙적으로 안전하다는 사실이 이론적으로 증명되었다 [15, 16]. 이론적으로 증명할 때 사용하는 몇 가지 가정이 있는데, 가장 중요한 가정은, 앨리스(Alice), 밥(Bob), 이브(Eve)의 시스템이 양자 이론의 지배를 받는다는 사실이다. 즉, 미시 세계의 물리학을 기술하는 양자 이론이 옳다는 가정 하에서 양자 키 분배의 보안성은 증명될 수 있다. 양자 키 분배에 대한 관심을 시작으로, 양자 상태를 정보론 관점에서 이해하려는 연구가 급속히 진행되었다. 암호학보다 더 넓은 관점인 통신 이론에서 양자 상태를 고려하고, 또한 통신 이론에 양자 상태를 적용하여 고전계로는 가능하지 않았던 정보 처리 과정들이 양자 계에서는 가능하게 됨을 보이기도 했다.

양자 키 분배를 실제로 구현할 때에는, 분배하는 양자 상태의 재료로서 광자의 편광을 사용한다. 광자는 주변 환경과 상호작용이 상대적으로 적어, 결맞음이 오래 동안 지속된다는 장점을 지니고 있으므로 현재로서 가장 적합한 양자 상태 전달의 매개체이다. 본 글에서는 양자 키 분배의 보안성에 대한 논의 중심으로 양자 키 분배의 이해 및 이론 연구를 간략히 정리하고자 한다. 이를 위해서 양자 키 분배의 과정을 소개한 후, 보안성에 대한 간략한 증명을 스케치하고 관련된 이론적 주제들을 논하겠다.

2. 큐빗과 양자 얽힘

양자 정보 이론에서는 양자 이론의 지배를 받는 물리계를 정보전달의 매개체로 사용한다. 정보이론에서 정보를 전달하는 단위가 0 혹은 1의 값을 가지는 비트 (bit) 상태였다면, 양자 정보 이론에서 정보의 단위는 에너지 준위를 두 개로 가지는 임의의 모든 입자가 될 수 있다. 이를 흔히, 양자 비트 (quantum bit)라고 하고 줄여서 큐빗 (Qubit)이라고 한다. 이진수 값 0 (1)을 두 에너지 준위의 고유벡터들인 $|0\rangle$ ($|1\rangle$)으로 대응하자. 그렇다면, 큐빗의



양자 상태는 두 상태 $|0\rangle$과 $|1\rangle$의 임의의 중첩이 될 것이다. 이는 블로흐 구 (Bloch sphere)라고 불리는 구의 한 점으로 표현될 수 있다.

양자 얽힘은 두 개 이상의 입자들의 상태를 기술할 때 나타나는데, 양자 상태에 있는 입자들 사이에 존재하는 양자 상관 관계(quantum correlations)이다. 이러한 상관 관계는 고전계들이 지니는 상관관계(classical correlations)로 설명할 수 없다. 개개의 입자들의 상태들을 조합해서 전체 양자 상태를 묘사할 수 없을 때, 양자계는 양자 상관관계를 지니고 있다고 하거나 혹은 얽혀(entangled) 있다고 한다. 얽혀 있지 않은 상태들은 고전계들이 갖는 상관관계만을 갖고 있다. 예를 들어, 두 개의 입자 A와 B가 있다고 할 때, 각각의 입자들의 상태는 ρ_A 및 ρ_B 로 표현된다고 하자. 전체 상태 ρ_{AB} 가 국소 상태들로만 생성된 $\rho_A \otimes \rho_B$ 의 상태 혹은 그들이 어떠한 고전계들의 상관관계 (통신을 통하여 준비될 수도 있는)들로만 묘사될 수 있는 경우, (즉, 다음처럼 표현할 수 있다)

분리가능한 상태들의 표현: $\sum_i p_i \rho_A^i \otimes \rho_B^i$

전체 상태는 분리 가능한(separable) 상태라고 한다. 그렇지 않은 경우에 대해서, 전체 상태는 얽혀있다고 한다. 양자 얽힘은 고전계가 흉내 낼 수 없다. 얽힌 상태의 대표적인 예로는 양자 상태 $|\phi_1\rangle_{AB} = (|00\rangle + |11\rangle)/\sqrt{2}$ 인데, 이 상태를 포함한 다음 세 개의 상태들은 최대로 얽힌 상태 (maximally entangled states)들이며 벨 상태들이라고 부른다:

$|\phi_2>_{AB}=(|00>-|11>)/\sqrt{2}$,
$|\phi_3>_{AB}=(|01>+|10>)/\sqrt{2}$,
$|\phi_4>_{AB}=(|01>-|10>)/\sqrt{2}$.

주어진 양자 상태가 얽혀 있는지 혹은 분리 가능한 지를 판별하는 문제는 매우 어려운 것으로 알려져 있으며, 일반적인 해법은 양의 변환 함수(positive map) Λ을 양자 상태에 적용하는 것이다. 양의 변환 함수는 양자 상태를 다른 양자 상태로 변환한다. 그러나 이는 실제로 물리적인 변환은 아닌데, 그 이유는 전체 계의 부분 계에만 취했을 경우 부분 계는 양자 상태일 수 있으나 전체 계는 물리적으로 해석이 어려운 음의 기대치를 제공할 수가 있기 때문이다. 양자 계에 대해서 양의 변환 함수가 고전계와는 다르게 이러한 성질을 갖게 되는 이유는 양자 이론에서 얽힌 양자 상태들이 존재하기 때문이다.

그럼에도 불구하고, 특정한 범위의 양자 상태에 대해서는 주어진 상태가 얽혀 있는지 혹은 분리가능한지를 판별하는 방법이 알려져 있다. 두 개의 큐빗 상태에 대해서는, 양의 변환 함수 중에 하나인 전치 변환 (transpose) 함수, T 는 상태가 얽혀 있는 분리가능한 지에 대한 대답을 정확히 제공한다. 벨 대각화 상태라고 불리는 다음의 상태가 얽혀 있을 조건을 살펴보자,

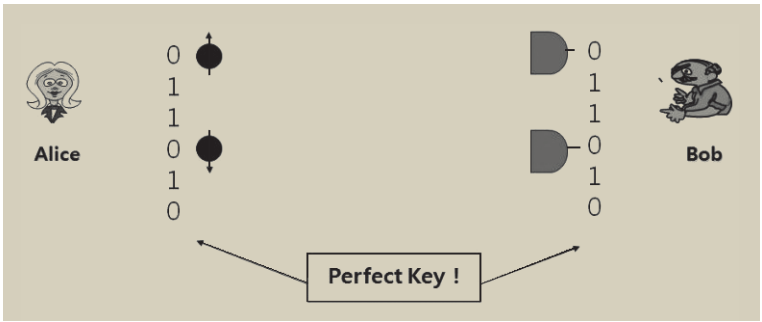
벨 대각화 상태:
$\rho_{AB}-\lambda_1|\phi_1><\phi_1|+\lambda_2|\phi_2><\phi_2|+\lambda_3|\phi_3><\phi_3|+\lambda_4|\phi_4><\phi_4|$.

벨 대각화 상태에 전치 변한 함수를 취하게 되면, $(I_A\otimes T_B)[\rho_{AB}]$ 으로부터, 네 개의 고유치는 $(-\lambda_1+\lambda_2+\lambda_3+\lambda_4)/2$, $(\lambda_1-\lambda_2+\lambda_3+\lambda_4)/2$, $(\lambda_1+\lambda_2-\lambda_3+\lambda_4)/2$, $(\lambda_1+\lambda_2+\lambda_3-\lambda_4)/2$ 으로 얻게 되고, 양자 상태가 규격화 되어 있다는 조건, $\lambda_1+\lambda_2+\lambda_3+\lambda_4=1$ 으로부터, λ_1, λ_2, λ_3, λ_4 중 어느 하나만이라도 1/2 보다 크면 ρ_{AB} 는 얽힌 상태라고 결정할 수가 있다. 예를 들어, 상태 $|\phi_1>_{AB}=(|00>+|11>)/\sqrt{2}$ 의 B 시스템에 전치 변환 함수를 적용하면 고유치들은 1/2, 1/2, 1/2, -1/2 이므로 음의 기대치의 존재를 통해서 얽힌 상태임을 판별할 수 있다 [7].

일반적으로 임의의 차원의 양자 상태 ρ_{AB} 가 얽혀 있는지 분리 가능한 지를 판별하는 과정은 다음과 같다. 특정 양의 변환 함수 Λ 를 부분계에 취한 후, $(I_A\otimes\Lambda_B)[\rho_{AB}]$ 으로부터, 물리적으로 해석할 수 없는 음의 기대치가 존재하는 지를 분석해서, 존재한다면 상태 ρ_{AB} 는 얽혀 있다고 결정할 수 있다. 그 역으로, 상태가 얽혀 있다면, 음의 기대치를 제공하는 양의 변환 함수가 존재한다. 즉, 얽힌 상태의 존재와 양의 변환 함수의 존재는 필요 충분 조건이다. 이와 같은 일반적인 방법이 알려져 있음에도 불구하고, 이 문제가 일반적으로 어려운 이유 중 하나는, 양의 변환 함수들의 성질들에 대한 이해가 아직 부족하기 때문이며, 양의 변환 함수에 대한 연구는 수학에서 오랫동안 연구되고 있는 분야이기도 하다 [2].

3. 양자 키 분배 프로토콜

BB84은 양자 키 분배 프로토콜 중 가장 먼저 개발되었는데, 그럼에도 불구하고 양자 키 분배의 대표적인 프로토콜이라고 할 수 있다. 후에 D. Bruss에 의해서 six-state 프로토콜로 일반화 되었다 [8]. A. Ekert는 1991년 양자 얽힘에 기반을 둔 E91 프로토콜을 개발하였는데, 이는 양자 얽힘이 비국소성을 지닌다는 아이디어에 기인하고 있다 [9]. 1992년 C. Bennett, G. Brassard, N. D. Mermin은, 앞서 언급한 모든 프로토콜들이 양자 얽힘 기반의 프로토콜 (Entanglement-based scheme)로 전환될



수 있음을 보였다. 위에서 언급한 각각의 프로토콜자체를 통신의 한 방법으로 소개하는 논문이나 글들은 많이 있으므로, 여기서는 양자 키 분배 프로토콜을 양자 얽힘의 관점으로 설명하고자 한다. 특별히, BB84 및 six-state 프로토콜을 예로 들겠다.

먼저 실험으로 구현 가능한 방법인, 준비- 및-측정 방식(Prepare-and-measure scheme)으로 BB84를 설명하자. BB84 프로토콜에서는 네 개의 기저를 이진수 값 0과 1을 전송하는 데 사용한다. 네 개의 기저는 큐빗의 z 축의 직교 기저 $Z=\{|0>_z,|1>_z\}$ 와 x 축의 직교 기저 $X=\{|0>_x,|1>_x\}$이다. 앨리스(Alice)는 Z 및 X의 집합에서, 0의 값을 $|0\rangle$ 상태에 대응하고 1의 값을 $11\rangle$ 상태에 대응시켜서, 양자 상태를 보낸다. 이 때 앨리스(Alice)의 Z 및 X 기저를 선택은 무작위(random)로만 한다. 만일 도청자가 기저의 선택을 예측할 수 있다면, 도청자는 그에 대응하는 직교 기저를 선택해서 측정하여 앨리스(Alice)가 보내고자 했던 값들을 쉽게 얻을 수 있을 것이다. 앨리스(Alice)가 기저를 무작위로 선택하여 상태를 전송한 후에, 밥(Bob)은 기저 Z 및 X를 임의로 바꾸어 가며 측정한다. 이 때, 밥(Bob)의 선택이 우연히 앨리스(Alice)의 선택과 일치할 경우 앨리스(Alice)와 밥(Bob)은 완벽한 값을 공유하게 되지만, 그렇지 않다면, 정확히 같은 값을 나눠 가지지 못할 것이다. 양자 상태 측정 후에, 앨리스(Alice)는 자신이 선택했던 기저들이 X 인지 Z 인지를 밥(Bob)에게 발표하는데 이 과정은 도청자에게 노출되어도 상관없다. 도청자는 자신이 이전에 정했던 기저로 이미 상호작용을 끝낸 후이기 때문에 그 후에 측정 기저를 알게 된다 하더라도 앨리스(Alice)와 밥(Bob)의 관심 대상이 되는 측정 데이터를 알게 된다는 것 이외에) 더 새로운 정보를 얻을 수는 없다. 그래서 밥(Bob)은 기저가 일치하지 않는 경우를 모두 걸러내어 기저가 일치하는 경우만 앨리스(Alice)에게 알려 주어서 두 당사자의 기저 선택이 일치하는 경우에 측정한 값들만 모은다. 이 과정을 키 거름 과정(sifting)이라고 하고 키 거름 과정 이후에 얻은 측정값들을 "걸러진 키들(sifted raw key)"이라고 부른다. 양자 키 분배는 이러한 걸러진 키들로부터 고전 통신 기술들, 오류 수정 및 보안성 증폭 과정 (error-correction and privacy amplification)의 기술들을 통해서 비밀 키를 얻어내는 과정이다. Six-state 프로토콜은 BB84에 $Y=\{|0>_y,|1>_y\}$ 기저를 BB84의 네 개의 기저에 더 포함한 프로토콜이며, 나머지 과정은 BB84와 동일하다.

양자 키 분배 프로토콜이 고전 프로토콜과 다른 점은 상태 분배 과정에서 양자 상태에 0과 1의 값을 대응시켰다는 점이다. 이는 다음의 사실을 의미한다. 첫 번째는 앨리스(Alice)와 기저의 선택이 일치하는 사람만이 양자 앨리스(Alice)가 대응시켰던 값들 0 혹은 1의 값을 얻어낼 수 있다는 점이다. 더욱 중요한 사실은, 주어진 양자 상태가 어떤 상태인지 알지 못하는 상황에서 그 양자 상태에 대한 정보의 증폭은 불가능하다. 그 양자 상태를 복사하거나 혹은 상태가 무엇인지에 대한 정보를 증폭하는 일은 불가능하다. 이는 고전 물리계의 상태들과 구별되는 성질이며, 전파 불가능(no-broadcasting) 혹은 복제 불가능 정리(no-cloning) 라고 한다. 가령, 고전 물리학의 경우 종이에 씌여진 글이 무슨 내용인지 보지 않았다 하더라도 그 종이에 씌여진 내용을 복제하는 방법이 있다. 하지만, 양자계의 상태들을 이용하여 정보를 표시했고, 그 내용을 알지 못한다면, 그 정보를 완벽히 복제하는 방법은 존재하지 않는다. 복제 불가능 정리가 양자 키 분배에서 의미하는 바는 다음과 같다. 앨리스(Alice)가 X 및 Z의 상태를 임의로 선택하여 보냈을 때, 도청자가 그 상태를 알기 위해서 약한 상호작용을 했다고 하면, i) 도청자는 어느 양자 상태인지 정확히 알지 못하므로 그 양자 상태에 대한 정보를 증폭하는 것이 불가능하고 따라서 어느 상태인지에 대한 정보를 모두 얻을 수 없으며, ii)약간의 상호작용으로 인하여 앨리스(Alice)가 보냈던 초기 상태는 변하게 되었으므로 밥(Bob)은 자신의 상태가 얼마나 변했는지를 확인하여 도청자가 어떻게 어느 정도 관여했는지를 측정 데이터를 통해서 알아낼 수가 있다. 즉, 도청자의 흔적이 밥(Bob)이 받는 상태에 남는다는 것을 의미한다.

양자 얽힘 기반의 프로토콜. 위의 프로토콜들을 동일한 과정인 양자 얽힘 기반의 프로토콜로 이해할 수 있다 [11]. 앨리스(Alice)는 최대로 얽힌 상태 $|\phi_1>=(|00>+|11>)/\sqrt{2}$ 를 생성한다. 앨리스(Alice)는 첫 번째 입자를 측정하는데 이 때 0의 값이 측정될지 1의 값이 측정 될지는 양자 이론의 성질대로 무작위(random)로 주어진다. 이를 양자 상태에 원칙적으로 존재하는 무작위성 (quantum randomness)이라고 하는데, 이러한 성질 때문에 앨리스

양자 키 분배의 이론

(Alice)가 0과 1의 값을 무작위로 생성하는 과정을 상태 발생과 측정으로 대신할 수 있다. 그 후 앨리스(Alice)는 두번째 입자를 밥(Bob)에서 보내는데, 보내는 과정에서 두 번째 입자는 주변의 모든 환경을 포함한 도청자와 약한 상호작용(근사적인 양자 상태 복제과정)을 하게 된다. 그 결과 앨리스(Alice)가 보낸 상태에 에러들이 존재하게 되고 에러가 존재하는 상태(corrupted state)를 밥(Bob)은 받게 된다. 그러한 에러들은 $|0\rangle$ 상태를 $|1\rangle$ 상태로 변환하거나 혹은 $|1\rangle$ 상태를 $|0\rangle$ 상태로 변환하는 비트에러(bit-error)가 있고, 상태 $|+>=(|0>+|1>)/\sqrt{2}$ 를 $|->=(|0>-|1>)/\sqrt{2}$ 로 변환하거나 혹은 $|->=(|0>+|1>)/\sqrt{2}$ 상태를 $|+>=(|0>+|1>)/\sqrt{2}$ 로 변환하여 위상에 에러를 발생시키는 위상에러 (phase-error)이다. 물론 더 일반적인 에러들이 생길 수는 있으나, 그러한 에러들은 앨리스(Alice)와 밥(Bob)의 국소 작용을 통해 제거하여 위의 두 가지 종류의 에러들로 귀결시킬 수 있다. 따라서, 앨리스(Alice)와 밥(Bob) 사이의 양자 상태는 에러 생성 확률에 의해서 다음의 벨 대각화 상태가 될 수 있는데,

$$\rho_{AB}=\lambda_1|\phi_1><\phi_1|+\lambda_2|\phi_2><\phi_2|+\lambda_3|\phi_3><\phi_3|+\lambda_4|\phi_4><\phi_4|$$

여기서 비트에러의 비율은 다음과 같이 계산할 수 있고,

$$<01|\rho_{AB}|01>+<10|\rho_{AB}|10>=\lambda_3+\lambda_4$$

위상에러의 비율은 다음과 같이 계산할 수 있다,

$$<+-|\rho_{AB}|+->+<-+|\rho_{AB}|-+>=\lambda_2+\lambda_4$$

앞에서 설명한 BB84 프로토콜과 six-state 프로토콜에서는 비트에러의 비율과 위상에러의 비율이 같고, 그 값을 양자에러비율 (Quantum Bit Error Rate-QBER)이라고 부른다. BB84 프로토콜은, X기저와 Z 기저는 측정의 대칭성을 지니고 있으므로, 앨리스(Alice)와 밥(Bob)이 각각 Z 축으로 측정했을 때와 X 축으로 했을 때, i) 같은 값의 양자 에러 비율 (QBER)을 얻어야 하며 ii) 또한 같은 값의 성공 비율을 얻어야 한다. 이 두 가지 조건들과 양자 상태는 규격화 되어 있다는 세 가지 조건으로 BB84에 대응하는 네 개의 변수 λ_1, λ_2, λ_3, λ_4 들을 하나의 자유 변수 x 와 양자 에러 비율 값 $q=\lambda_3+\lambda_4$ 두 가지로 결정할 수 있다 [11]:

$$\lambda_1=1-2q-x\ ,$$
$$\lambda_2=\lambda_3-q-x\ ,$$
$$\lambda_4=x\ .$$

여기서, 자유 변수 x 는 앨리스(Alice)와 밥(Bob)의 양자 에러 비율(QBER)에 측정되지 않는 양으로서 도청자가 임의대로 결정할 수 있는데, 보안성 증명을 위해서는 앨리스(Alice)와 밥(Bob)이 비밀 키를 나눠 갖지 못하는 최적의 값으로 결정한다고 가정한다. Six-state 프로토콜의 경우는, Y축에 대한 대칭성을 더 추가함으로서 네 개의 조건을 갖게 되며, 네 개의 변수를 정확히 결정할 수 있게 된다.

양자 얽힘 기반의 프로토콜 방식으로 BB84와 six-state 프로토콜들을 변환했을 경우, 보안성에 대한 성질은 양자 상태의 얽힘과 관련한다. 앨리스(Alice)가 최대로 얽힌 상태를 만들어 한 입자를 보내고, 도청자가 그 입자와 자신의 입자가 얽힌 상태에 있도록 작용한다면, 밥(Bob)이 앨리스(Alice)와 나눠가진 상태의 얽힘 정도는 도청자와 앨리스(Alice)의 상태의 얽힘 정도만큼 감소하게 된다 [12]. 즉, 한 사람 앨리스(Alice)가 양자 얽힘을 다른 여러 사람들과 나눠 같고자 할 경우, 앨리스(Alice)가 각 사람 개별과 나눠 가진 양자 얽힘의 정도는 약화된다. 이를 양자 얽힘의 일부일처 성질 (monogamous)이라고 한다 [13]. 양자 키 분배에서는 양자 얽힘의 이러한 성질이 반영되는데, 앨리스와 밥은 양자 에러 비율을 통해서 이를 확인할 수 있다. 에러 비율이 너무 크다면, 둘 사이의 양자 얽힘 정도가 작다는 뜻이며, 에러 비율이 매우 작다면 둘 사이의 양자 얽힘의 정도는 충분히 크다는 뜻이다. 그렇다면, 보안성을 의미하는 양자 에러 비율의 크기는 얼마일지 알아보자.

4. 양자 키 분배의 보안성

위의 양자 키 분배 과정을 구현했다고 했을 때, 양자 상태를 전송하고 측정 후에 남는 것은 최종적으로 걸러진 키(sifted raw key)이며, 이들은 특정 확률 분포를 지닌 이진수 0과 1의 데이터이다. 여기서, 앨리스(Alice)와 밥(Bob)이 나눠 가진 상태를 ρ_{AB} 으로 알고 있다고 했을 때, 확률 분포는 $P(A,B)=tr[\rho_{AB}M_A\otimes M_B]$ 으로 주어질 것이며 여기서 $M_{A(B)}$ 는 앨리스(Alice)와 밥(Bob)의 측정 연상자이다. 여기서 상태 ρ_{AB} 가 얽힌 양자 상태가 아니라면, 즉 분리 가능한 상태라면 키 분배는 성립될 수 없다. 왜냐하면 $P(A,B)$ 에서 앨리스(Alice)와 밥(Bob)이 서로 독립시행이 되거나 혹은 독립시행들의 조합으로 표현될 수 있으므로 고전 암호학의 확률 분포와 동일해 지게 된다, 결국, 도청자는 밥(Bob)이 얻을 수 있는 정보만큼 얻을 수 있음을 의미하게 되며, 키는 생성할 수 없게 된다. 그러므로, 양자 얽힘은 양자 키 분배가 가능하게 되는 필요조건이다.

양자 상태 분배 및 측정 후의 과정은 고전 암호학에서 사용하는 후처리 (에러 수정와 보안성 증폭 과정)이며 이를 통해서 최종적으로 보안성을 증명할 수 있게 된다. 가령, 다음의 측정 데이터가 있다고 하자:

A	B	
1	1	(a)
0	0	(b)
0	1	(c)
1	1	(d)

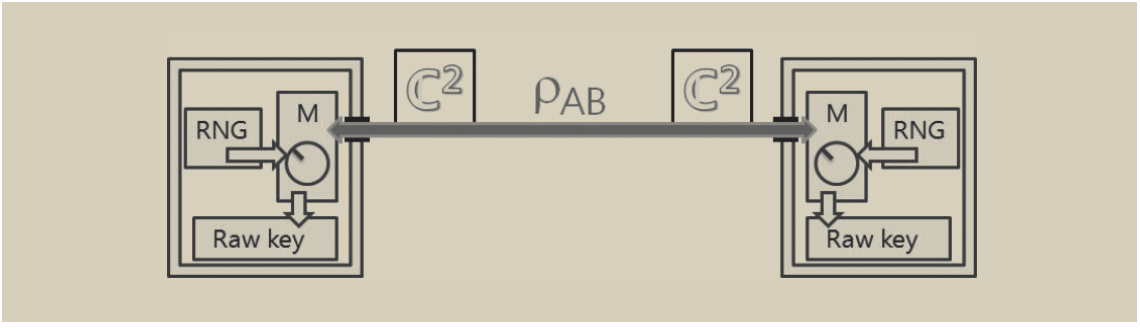
A는 (a)와 (b)의 값들을 더한 1의 값을 B에게 알려 준다. B는 자신의 값이 0과 1을 더한 1임을 알려 주지 않고 기록만 한다. A는 다시 (b)와 (c)를 더하고 0임을 알려준다. B는 자신의 경우가 1임을 기록해 두고, (b)와 (c) 중에 에러가 존재함을 기억하지만 어느 것인지는 모른다. 앨리스(Alice)는 (a)와 (d), (c)와 (d)에 대해서 같은 방법을 취하는데, 이를 통해서 밥(Bob)은 자신의 (b)의 값에는 에러가 없음을 확신하고 (c)의 값을 1에서 0으로 수정한다. 이는 단방향 에러 수정의 한 예이며 실제로는 더욱 복잡한 에러 수정 코드가 사용된다. 1978년에 I. Csiszar와 J. Korner는 앨리스(Alice)와 밥(Bob)이 공유한 정보, I(A:B)가 앨리스(Alice)와 이브(Eve)가 공유한 정보 I(A:E) 보다 더 많을 때,

$$I(A:B) > I(A:E)$$

으로 표현할 수 있으며, 단방향 후처리를 통하여 비밀키를 만들어 낼 수 있음을 보였다. 이를 Csiszr-Korner 정리라고 한다 [14]. 여기서 I(A:X)는 A와 X가 지닌 교류정보(mutual information)이며, 이는 확률 분포 $P(A,B)$ 로부터 얻을 수 있다.

도청자 이브(Eve)가 양자 상태를 언제 측정하는 지의 여부는 양자 키 분배에서 중요하다. 도청자가 측정을 했다면 I(A:E)는 확률 분포로부터 얻을 수 있으므로 위에서의 Csiszr-Korner 정리를 이용하여 키를 얻을 수 있는 양자 상태의 조건을 구해낼 수 있다. 이 경우 보안성을 제공하는 양자 에러 비율(QBER)은 약 14%로 알려져 있다. 즉, 양자 에러 비율이 14% 이하일 경우에만, 앨리스(Alice)와 밥(Bob)은 단방향 후처리 통신을 사용하여 키를 얻을 수 있다.

측정하지 않고 양자 상태를 보관함으로 기다리고 있다면, 고전 (앨리스(Alice)는 측정 후 이므로)-양자 (도청자는 양자 상태를 보관하고 있으므로) 상태 간의 공유 정보 I(A:E)를 정량화할 양이 필요하다. 소위 Holevo



quantity에서 I(A:E)를 얻어낼 수 있는데, Holevo quantity는 주어진 양자 상태로부터 얻을 수 있는 최대의 고전 정보량을 정량화 한다. 도청자가 양자 상태에 머물 때에 키 생성에 대한 조건은 I. Devetak과 A. Winter, 그리고 R. Renner에 의해서 각각 독립적으로 보여졌다 [15,16]. 이는 양자 키 분배에서 가장 일반적인 보안성을 증명하는 과정이다. 이 증명과정을 BB84에 적용했을 때, 보안성을 제공하는 QBER는 11% 이하의 범주에 있다 [17]. 즉, 앨리스(Alice)와 밥(Bob)이 raw key 로부터 QBER를 측정했을 때 11% 이하였다면, 단방향 키 생성 방식을 통해서 키를 생성해 낼 수 있다. 그러나, 11% 이상의 QBER 가 안전하지 않다는 뜻은 아니다. 다만, 안전한 지 안전하지 않은 지 아직 대답할 수 없음을 뜻한다. 최근, 11%를 발전시켜 12.4% 까지 증명되었고 [18], 그 후 12.8% 까지도 보여졌다 [20]. 그러나 이러한 값들이 더 이상 발전하지 못하는 지 역시 알려지지 않았다. 단방향보다 더 일반적인 양방향 통신을 사용할 경우, 20% 까지도 안전함이 알려져 있으나, 20% 이상으로 더 발전하지 못하는 지에 대한 여부도 알려져 있지 않다 [21].

5. 양자 키 분배를 위한 가정들

양자 키 분배를 위한 과정을 다시 살펴보면, 앨리스(Alice)와 밥(Bob) 및 도청자 이브(Eve)가 양자 이론에 의해서 지배된다는 사실 이 외에도 몇 가지 실제적인 가정이 더 있다. 양자 키 분배를 구현하는 문제는 양자 이론만의 일은 아니기 때문이다. 이러한 가정들은 정말로 안전한 양자 키 분배 장치를 현실에서 갖게 될 수 있는 지에 대한 여부에 관한 중요한 주제일 뿐 아니라, 물리계를 포괄적으로 이해하는데 새로운 방법을 제시하기도 한다. 그러한 가정들을 하나씩 살펴보자 [3].

i) 실험실의 장치의 국소화 문제

첫 번째로 양자 키 분배를 하는 두 실험실이 멀리 떨어져 있다고 했을 때, 각 실험실의 장치들은 도청자의 장치와 독립적이어야 한다. 혹은 각 실험실의 장치들이 수행하는 작업의 어떤 신호도 실험실 밖을 나가서 어떠한 작업이 진행 중인 지에 대한 정보를 제공해서는 안 된다. 이렇게 정보가 세어나가게 되면, 그 정보를 이용하여 도청자는 새로운 공격을 할 수 있게 된다. 그렇다면, 앞서 했던 증명이 유효하지 않다. 이는 물리학의 일반적인 가정인 국소성 (locality) 가정과 관련이 있다.

이를 해결하기 위해서는, 앨리스(Alice)의 어떤 장치도 외부에 정보를 제공하지 않음을 증명해야 한다. 혹은, 어떤 고전적인 정보가 세어나가서 이브(Eve)의 도청에 도움을 준다 하더라도, 양자 키 분배가 안전하다는 것을 증명해야 한다.

ii) 0과 1의 무작위(random) 생성 문제

앨리스(Alice)는 0과 1의 값을 무작위로 생성해 내야만 한다. 값들이 어떠한 주기적 성질을 지니고 있다는 사실이 드러난다면 이브(Eve)는 그러한 정보를 통해서, 측정 기저를 예측할 수 있게 되어, 위의 보안성 증명이 더 이상 유효하지 않게 된다. 이 문제는 앞서 설명한 측정 장치의 국소화 문제와도 관련된다.

iii) 사용하는 양자 상태의 차원 문제

앨리스(Alice)와 밥(Bob)은 양자 상태를 생성하고 측정할 때, 자신들의 상태가 2차원의 상태, 즉 큐빗이라고 가정한다. 더욱 고차원의 상태가 생성되어 전송한다고 해도, 밥(Bob)은 2차원의 값들로만 측정하고 해석할 것이다. 만일 앨리스(Alice)와 밥(Bob)이 구입한 장치를 만든 사람이 도청자 이브(Eve)였고, 도청자 이브(Eve)는 장치가 몰래 2차원 이상의 양자 상태를 생성하도록 만들었다면, 2차원을 가정하고 보안성을 증명한 위의 증명은 더 이상 유효하지 않다. 이러한 시나리오를 가정하는 이유는, 앨리스(Alice)와 밥(Bob)이 궁극적으로 보안성을 얻고자 하기 때문이며, 사용하는 장비에 대한 신뢰도는 보안성의 증명에 중요하기 때문이다.

이 문제를 해결하기 위해서는, 앨리스(Alice)와 밥(Bob)은 자신들의 양자 상태가 존재하는 힐버트 공간의 크기를 분석해 낼 수 있는 방법을 찾아야 한다. 실제로, 벨 부등식은 차원에 따라 위반하는 정도가 다르다. 이 사실을 이용하여, 힐버트 공간의 크기 측정 문제의 부분적인 결과가 존재한다 [19].

iv) 단광자 생성의 문제

위의 가정들을 다 수용한다고 하더라도, 실제 실험에서 단광자를 생성하여 전송하는 것은 쉽지 않다. 레이저 빛을 충분히 약화 시켜 평균 광자 개수를 약 0.1 – 0.2개 정도로 조절한 후에 빛을 내 보낸다 하더라도, 두 개의 광자가 생성될 확률은 여전히 존재한다. 광자가 두 개 이상 전송되게 되면, 도청자는 광자 개수를 세는 방법을 통해 공격하는 방법을 생각하게 되는데, 이를 광자 개수 분리 (Photon Number Splitting) 공격이라고 한다. 이 공격에서는, 광자의 개수가 1개이면 도청자는 중간에서 막고 전송되지 않도록 한다. 두 개 이상이면 도청자는 하나만 보내고 다른 하나는 저장하여 기다리다가 앨리스(Alice)가 측정 기저를 발표할 때 동시에 측정한다. 이렇게 한다면, 앨리스(Alice)의 정보는 여러 정보로 나눠질 수 있게 되어서, 위의 증명이 유효하지 않다.

이 문제는 실험 장치의 불완전한 부분이므로, 훗날 단광자를 생성해 내는 장치가 개발된다면 해결될 것이다. 흥미롭게도, 실험의 불완전한 부분을 이론적인 개선으로 보완할 수 있음이 다음의 두 결과에 의해서 보였다. 전남대학교 황원영 교수님께서 개발한 미끼를 이용한 방법 (Decoy state) [22] 과 (키 분배에서 미끼가 되는 채널을 포함시킨다), 제네바 그룹(V. Scarani, A. Acin, G. Ribody, N. Gisin)에서 BB84의 sifting 과정을 변형하여 개발한 Scarani-Acin-Ribody-Gisin (SARG) 04 프로토콜이다 [23].

6. 장치 독립적 양자 키 분배

양자 키 분배의 모든 증명과정에서는 양자 이론이 미시세계를 묘사하는 이론으로 가정하였으나, 양자 이론이 옳은 이론인지 알 수 없으며, 다만 현재까지 양자 이론의 실험 결과들을 잘 예상하고 있다는 것으로 양자 이론을 간주할 뿐이다. 만일, 양자 키 분배가 양자 이론 뿐 아니라 그 이상의 다른 물리학 이론에서도, 혹은 미래에 알게 될 물리학의 새로운 이론의 지배하에서도, 여전히 안전할 지는 물리적으로 흥미로운 주제이다. 최근 이에 대한 연구가 진행 중인데, 이를 장치 독립적 양자 키 분배 (Device-independent Quantum Key Distribution) 프로토콜 이라고 한다 [24].

장치 독립적 양자 키 분배 프로토콜의 과정은 양자 키 분배 과정과 동일하다. 차이점은, 벨 부등식을 위반할 때 사용하는 기저들로서 BB84를 구성하며, 보안성을 증명하는 데 있어서는 장치 독립적 양자 키 분배에서는 양자 이론에서 양자 상태들의 공간으로 가정하고 있는 힐버트 공간을 고려하지 않는다. 앞서서 언급했던 가정들 중 양자 상태들의 차원도 가정하지 않는다. 또한, 측정 장치가 어떠한 정보를 이브(Eve)에게 주는 지도 신뢰하지 않는다. 다만, 양자 상태를 생성했다고 가정하고 이를 통해서 측정 값의 확률 분포 $P(AB|\mu_{AB})$를 얻을 수 있다고 가정하고 그 확률분포만을 신뢰한다. 실험을 통해, 양자 이론을 고전 세계에서 볼 수 있는 방법 중 하나는 바로 확률 분포이므로 이러한 가정은 좀 더 실제적이라 할 수 있다. 그러나, 광학 실험에서의 측정 문제 (detection loophole)로 인해서 확률 분포 $P(AB|\mu_{AB})$를 정확히 신뢰할 수 있는 지는 여전히 가정으로 남아 있으며. 또한, 앞서서 언급한 0과 1의 무작위(random) 생성 문제 역시 해결하지는 못하고 있다.

장치 독립적 양자 키 분패 프로토콜은 양자 이론보다 더 일반적인 이론을 가정한 후 얻어진 확률 분포만을 신뢰하므로, 물리적으로 흥미있고 의미있는 연구이다. 또한, 양자 이론의 근간이 되는 비국소성 논의에 직접적 관련이 있기도 하다. 그러나, 현재까지도 장치 독립적 양자 키 분배 프로토콜의 가장 일반적 보안성은 증명되지 않았다. 비국소성(벨 부등식의 위반)이 보안성의 필요조건이라는 결과가 알려져 있다 [25]. 즉, 확률 분포 $P(AB|\mu_{AB})$ 가 벨 부등식을 위반하지 않는다면, 다시 말해서, 두 당사자 앨리스(Alice)와 밥(Bob)의 확률 분포를 설명하는 국소적 모델 (local model)이 존재한다면, 앨리스(Alice)와 밥(Bob)은 안전하지 않다. 이는 양자 키 분배와 대응하여 매우 흥미로운 관계를 보여 주고 있다. 양자 키 분배에서는, 앨리스(Alice)와 밥(Bob)이 나눠가진 상태 μ_{AB}의 얽힘이 앨리스(Alice)와 밥(Bob)의 보안성에 필요조건임이 알려져 있기 때문이다 [26]. 보안성을 위한 충분조건은, 흥미롭게도, 두 경우 모두에도 알려져 있지 않다.

	보안성을 위한 필요조건	보안성을 위한 충분조건
양자 키 분배	양자 얽힘	?
장치 독립적 양자 키 분배	비국소성(벨부등식 위반)	?

7. 양자 얽힘과 비밀 키의 인터페이스

양자 암호를 좀 더 일반적인 관점에서 본다면 다음의 과정으로 이해할 수 있다: 얽힌 양자 상태를 측정하여, 양자 얽힘이 측정값들의 상관관계로 얻어서, 그 상관관계를 비밀 키로 변환하는 과정이다. 여기서 도청자가 어떠한 능력을 가지고 있는 지를 제한하느냐에 따라, 보안성에 대한 조건과 증명이 달라진다. 도청자가 양자 상태를 저장하는 메모리가 없거나 혹은 있거나, 혹은 양자 이론보다 더 일반적인 다른 어떤 확률 분포를 제공하는 영역에 있거나 하는 등의 가정을 통해서 보안성의 분석과 조건이 달라진다.

양자 이론이 미시세계를 묘사하는 올바른 이론이라고 가정하자. 이 경우, 모든 양자 얽힘은 측정 후 유용한 고전 정보로 변환될 수 있는 것일까? 고전 이론과 양자 이론에서의 각각 상태들에서, 상태들 안에 존재하는 양자 및 고전 상관관계 (classical and quantum correlations)는 확연히 다르다. 여기서, 고전 상관 관계는 양자 얽힘 상태들을 사용하지 않고 시늉낼 수 있는 상관관계이며, 양자 상관 관계는 두 입자의 상관관계를 묘사할 때 양자 얽힘 상태들이 필연적으로 필요한 경우의 상관관계이다.

여러 입자들의 상태가 고전 상관관계만를 지닌다면, 그러한 양자 상태는 국소 준비 과정(local operations and classical communication)만으로 생성될 수 있으며, 따라서 그들의 확률 분포는 도청자가 언제가 알아 낼 수 있는 독립 시행들의 조합이다:

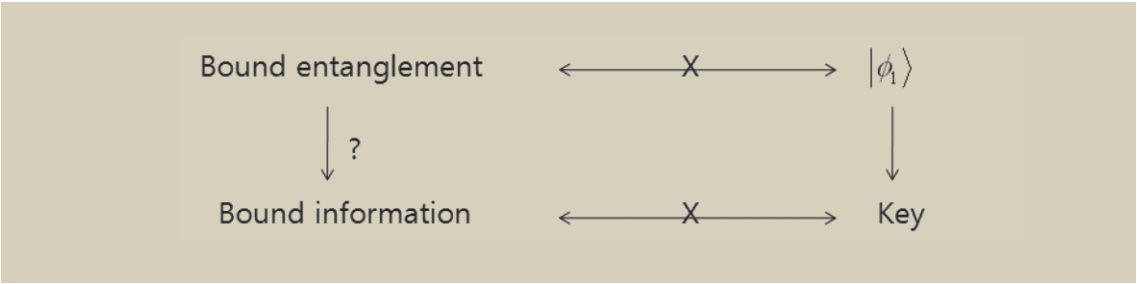
고전계를 통한 확률 분포
$P(A,B\|E)=\sum_i p_{ij}P_A(i\|E)P_B(j\|E)$
얽힌 양자 상태의 측정을 통한 확률분포
$P(A,B\|E)\neq\sum_i p_{ij}P_A(i\|E)P_B(j\|E)$

$$P(A,B|E)=\sum_{i,j} p_{ij}P_A(i|E)P_B(j|E).$$

얽힌 양자 상태를 측정할 경우, 위의 확률 분포처럼 되지 않도록 하는 측정 기저가 존재함이 알려져 있다. 다시 말하면, 양자 상태가 분리가능한 경우만 위의 확률 분포처럼 쓸 수 있고, 얽힌 상태의 경우 국소적 준비 과정만으로 준비할 수 없는 확률 분포를 제공한다.

따라서, 모든 얽힌 양자 상태은 측정을 했을 때 상관관계를 보여 주는데, 그 상관 관계는 고전계들의 국소 준비 과정 (local operations and classical communication)만으로 시늉낼 수 없는 상관관계를 지닌 확률 분포이다. 그러한 확률 분포가 비밀 키로 사용될 수 있을까? 혹은 정보 이론에 어떻게 쓸모 있을까? 만일 얽힌 상태를 측정해서 비밀 키를 얻어낼 수 없는 양자 상태가 존재한다면, 자연계에는 갇힌 정보 (bound information)이 존재한다는 것을 뜻한다. 특정 상관 관계(classical correlations)가 자연계에 존재하지만, 비밀 키로서 사용할 수 없도록 갇혀 있다면 그것은 무엇을 의미할까? 이는 여전히 진행 중인 연구 주제들이다. 흥미롭게도, 세 사람 이상 사이의 확률 분포에서 갇힌 정보는 존재함이 알려져 있다 [27]. 두 사람 사이의 갇힌 정보의 존재는 가설로 남아 있다.

고전 정보 이론에서 갇힌 정보의 존재는, 흥미롭게도, 양자 정보 이론의 갇힌 얽힌 상태 (bound entangled state)의 존재로부터 추측되었다. 갇힌 얽힌 상태는 국소 작용(local operations)들을 통해서 최대 얽힌 상태 (maximally entangled state)로 변환될 수 없는 얽힌 양자 상태들이다. 갇힌 얽힌 양자 상태를 준비하려고 하는 경우 최대 얽힌 상태들이 필요하지만, 그 역과정으로 갇힌 얽힌 상태들로부터 최대 얽힌 상태를 얻어내기는 불가능하다. 두 입자들이 갇힌 양자 상태에 있다는 것은, 과거 어느 시점 두 입자가 상호작용하여 얽히게 되었고 (entangled), 그 얽힘은 최대 얽힌 상태들로 변환되지 못



하는 것을 설명하는데, 이러한 현상이 물리계의 어떤 현상을 반영하여 의미하는 지에 대한 이해는 아직 부족하다.

8. 맺음말

양자 키 분배가 관심을 끌게 된 배경부터 양자 키 분배의 보안성, 최근의 연구 진행 상황 및 관련 연구 분야까지 간략히 살펴보았다. 기술적인 자세한 과정은 참조 논문 [1, 3, 11, 16, 18] 을 참고하기 바란다. 넓은 관점에서 양자 키 분배는 얽힌 양자 상태를 측정함으로 통해 얻은 확률 분포에서 비밀 키를 얻는 과정이다. 이러한 인터페이스의 측면에서, 양자 얽힘이 확률 분포에서의 상관관계와 어떻게 대응되는지 논의하였고 관련된 연구 주제들 또한 간략히 살펴보았다.

다음의 주제들은 본 글에서 포함하지 않았다. 보안성 증명에서 도청자가 제시하는 상호작용을 묘사하는, 양자 대칭 상태들 정리 (quantum de Finetti)는 본 글에서는 생략하였다 [16, 28]. 양자 키 분배와 관련된 양자 통신 용량 (quantum communication channel capacity)의 정보론적인 논의와 양자 상태들을 얽힌 정도에 관련된 내용도 제외하였다 [2]. 장거리 사이의 키 분배를 위해서는 양자 중계기 (quantum repeater)를 사용해야 하는데, 이에 대한 논의도 생략하였다. 자세한 관련 내용은 참조 논문 [2]와 [3]을 참고하기 바란다. 또한, 국소 환경이 키 분배 시스템과 고전적인 상관관계를 지니고 있는 경우의 양자 키 분배도 생략하였다. 이 경우에는 보안성 증명이 다소 다르다 [2].

양자 정보 이론은 물리계를 정보의 측면으로 해석함으로서 자연계에 대한 새로운 관점을 제시한다. 양자 정보 이론에서 연구하는 주제들 중, i) 양자 상태들의 정보론에 응용성 연구와 ii) 양자 이론을 측정한 측정값들의 정보론적 해석, 등을 기반으로 양자 키 분배의 보안성을 논의할 수 있다. 양자 키 분배는 양자 이론을 정보 이론에 직접적으로 적용하는 응용성을 지니고 있으며, 물리학 및 정보론 각각에서 가장 핵심적인 질문들, 가령 i) 자연계에 비국소적 숨은 변수 (non-local hidden variable)가 존재할 것인가 혹은, 자연은 비밀 공유를 원칙적으로 허락할 것인가, 그리고 ii) 비밀을 공유할 수 있도록 용납하는 자연계의 최소조건은 무엇인가, 등의 메세지를 포함하고 있다. 특별히, 장치 독립적 양자 키 분배에서 양자 이론에서의 도청자보다 더 일반적인 도청자를 가정함으로서, 양자 이론보다 더 일반적인 이론 (양자 상관관계보다 더 강력한 상관관계를 지닌다는 측면에서 더 일반적이다)에 대한 현재의 양자 키 분배의 보안성은 매우 흥미롭다. 또한 양자 이론을 포괄하는 새로운 이론을 얻는 방법에 대한 연구도 진행 중이다. 관련 실험들이 진행 중에 있으며, 최근에는 양자 얽힘의 실험을 통해서 비국소적 숨은 변수 (혹은 숨은 변수들 간의 비국소적 통신)는 존재하기 힘들 것이라는 실험적 증거와 설명이 제시되었다 [29].

흥미롭게도, 양자 이론을 정보 처리에 직접적으로 응용하고 있는 양자 키 분배에서, 1900년 양자 이론이 태동하던 시기에 양자 이론 근본에 대해 던져졌던 질문들이 다시금 고려되고 재해석되며 기존 물리학이 제시하지 못했던 양자 이론의 새로운 의미들을 보여주고 있다. 양자 키 분배의 연구는 양자 이론 및 물리학의 근본에 대한 질문 및 이해와 응용을 향한 연구를 동시에 수반한다. 양자 키 분배 연구에서는, 양자 이론을 정보 이론의 재료로서 적용하는 중이며, 물리학자들이 오랫동안 기대해 왔던 포스트 양자 이론 (post quantum theory)의 모습을 밝혀 가고 있는 중이다.

9. 감사의 글

본 글을 준비하는 데 조언을 주시고 교정을 도와주신 인하대학교 물리학과 김기식 교수님께 감사의 말씀을 드립니다.

참고문헌

[1] N. Gisin, G. Ribordy, W. Tittel and H. Zbinden, 2002, Rev. Mod. Phys. 74, 145.
[2] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, Rev. Mod. Phys. 81, 865 (2009)
[3] V. Scarani, H. B. Pasquinucci, N. J. Cerf, M. Dusek, N. Lutkenhaus and M. Peev, The Security of Practical Quantum Key Distribution, to appear Review of Modern Physics.
[4] P. Shor, *Proceedings of the 35th Annual Symposium on the Foundations of Computer Science, Santa Fe* (IEEE Computer Society, Los Alamitos), p. 124. (1994)
[5] C. Shannon, "Communication theory of secrecy systems", Bell System Technical Journal 28, 656-715 (1949).

양자 키 분배의 이론

〔6〕 C. H. Bennett and G. Brassard, "Quantum cryptography: public key distribution and coin tossing", Int. conf. Computers, Systems & Signal Processing, Bangalore, India, December 10-12, 175-179 (1984).
〔7〕 A. Peres, Phys. Rev. Lett. 76 1413 (1997); M. Horodecki, P. Horodecki, and R. Horodecki Phys. Lett. A 223 1 (1996)
〔8〕 D. Bruss, Phys. Rev. Lett. 81, 3018 (1998)
〔9〕 A. K. Ekert, Phys. Rev. Lett. 67, 661-663 (1991).
〔10〕 C. H. Bennett, G. Brassard, and N. D. Mermin, Phys. Rev. Lett, 68 557(1992).
〔11〕 M. Christandl, R. Renner and Artur Ekert, quant-ph/0402131 (2004).
〔12〕 V. Coffman, J. Kundu and W. K. Wootters, Phys. Rev. A 61, 052306 (2000).
〔13〕 B. M. Terhal, IBM J. Research and Development 48, 71 (2004).
〔14〕 I. Csiszar and J. Korner, Vol. IT-24, pp. 339-348, (1978).
〔15〕 I. Devetak and A. Winter, Phys. Rev. Lett. 93, 080501 (2004); R. Renner and R. Koenig, quant-ph/0403133.
〔16〕 R. Renner, Ph.D thesis
〔17〕 P. W. Shor and J. Preskill, Phys. Rev. Lett. 85, 441,(2000).
〔18〕 B. Kraus, N. Gisin, and R. Renner, Phys. Rev. Lett. 95, 080501 (2005); R. Renner, N. Gisin, and B. Kraus, Phys. Rev. A 72, 012332 (2005).
〔19〕 N. Brunner, S. Pironio, A. Acin, N. Gisin, A. A. Methot, V. Scarani, Phys. Rev. Lett. 100, 210503 (2008).
〔20〕 G. Smith, J. M. Renes, and J. A. Smolin, Phys. Rev. Lett. 100, 170502 (2008).
〔21〕 J. Bae and A. Acín, Physical Review A 75 012334 (2007); A. Acín et al., Physics Review A 73 012327 (2006).
〔22〕 W.-Y. Hwang, Phys. Rev. Lett. 91, 057901 (2003)
〔23〕 V. Scarani, A. Acin, G. Ribordy, and N. Gisin, Phys. Rev. Lett. 92, 057901 (2004).
〔24〕 A. Acin, N. Brunner, N. Gisin, S. Massar, S. Pironio, V. Scarani, Phys. Rev. Lett. 98, 230501 (2007).
〔25〕 J. Barrett, L. Hardy, and A. Kent, Phys. Rev. Lett. 95, 010503 (2005).
〔26〕 M. Curty, M. Lewenstein and N. Luetkenhaus, Phys. Rev. Lett. 92, 217903 (2004); A. Acin and N. Gisin Phys. Rev. Lett. 94, 020501 (2005).
〔27〕 Acin, A., J. I. Cirac, and L. Masanes, Phys. Rev. Lett. 92, 107903 (2004).
〔28〕 R. Renner, Nature Physics 3, 645 - 649 (2007).
〔29〕 D. Salart, A. Baas, C. Branciard, N. Gisin, H. Zbinden, Nature 454, 861-864 (2008).

약 력

배준우

• 약 력 :
2007 ~ 현재 : 고등과학원 연구원
2007 : Universitat de Barcelona, 물리학 (박사)
2003 : 한양대학교, 물리학 (석사)
2001 : 한양대학교, 수학 및 물리학 (학사)

• 주요경력 :
2003 – 2007 ICFO–Institute of Photonic Sciences (Barcelona)

• Email: jbae@kias.re.kr