情 報 保 護 學 會 誌
第 12 券 第 5 號, 2002. 10

양자 키분배 프로토콜

이 화 연*, 조 규 형*, 양 형 진**

요 약

양자 정보에 대한 도청은 양자 상태에 대한 측정이며, 양자역학에서의 측정은 양자 상태의 붕괴를 수반하게 되므로 원래의 정보 상태를 변형시키게 된다. 이를 이용하여 도청 시도의 여부를 거의 완벽하게 판단할 수 있으며, 따라서 고도의 보안이 유지되는 키분배 방식이 가능하게 된다. 이를 양자 암호 혹은 양자 키분배 프로토콜이라고 한다. 양자 역학의 기본 구조와 일반 원리를 제시하고, 이를 바탕으로 한 양자 암호의 기본 개념과 원리를 설명하고자 한다. 이에 대한 예로 대표적인 키분배 방식을 소개한다.

Ⅰ. 서 론

암호문의 안전성은 암호화와 복호화 과정에서의 안전성에 의존한다. 우리가 현재 사용하는 암호시스템은 암호화와 복호화를 위한 알고리즘이 공개되어 있지만 이러한 사실이 암호문의 안전성을 저해하지는 않는다. 이와 같은 암호체계에는 특별한 변수, 즉 키(key)가 사용되어, 평문과 함께 암호화 알고리즘의 입력값으로 들어가고, 암호문과 함께 복호화 알고리즘의 입력값으로 들어간다. 암호화, 복호화 알고리즘이 공개되어 있기 때문에, 암호문의 안전성은 전적으로 키의 안전성에 의존한다.

따라서 매우 중요한 역할을 담당하는 키는 충분히 긴 비트를 갖도록 무작위적으로 선택된다. 이 키를 설정하기 위하여, 어떤 비밀 정보도 공유하지 않은 두 사용자에게도 신뢰할 수 있고 안전한 채널이 필요하다. 고전 채널에서는 언제나 도청이 존재할 수 있고, 이를 합법적인 사용자가 확인할 수 없기 때문에 안전한 채널 확보는 기술적으로 꽤 어려운 일이다. 그러나 양자 역학의 고유한 특성을 활용하면 도청의 여부를 확인할 수 있기 때문에 안전하게 키를 공유할 수 있게 된다. 이렇게 양자 역학의 특성을 이용하여 안전하게 키를 분배하는 프로토콜을 양자 키분배 프로토콜이라고 한다.

이 논문에서는 양자 키 분배 프로토콜을 살펴보기 위하여 우선 양자 역학의 고유한 성질을 살펴보고, 지금까지 소개된 중요한 양자 키 분배 프로토콜을 소개하도록 하겠다.

Ⅱ. 양자 역학의 기본 원리

양자역학 고유의 현상에는 파동과 입자의 이중성(duality), 비연속성(discreteness), 측정에서의 양자 상태의 붕괴, 불확정성 원리, 양자 상태의 중첩(superposition), 양자상태의 얽힘(entanglement) 등이 있다.

파동과 입자라는 개념은 고전 물리학에서는 서로 배타적인 개념으로서, 파동이면 입자일 수 없고 입자이면 파동일 수 없다. 그러나 양자역학에서는 이 두 개념이 하나의 물체를 나타내는데 같이 사용된다. 이중성이란 동일한 물체라 할지라도 상황에 따라 파동의 측면을 드러낼 수도 있고 입자의 측면을 드러낼 수도 있다는 것을 의미한다.

비연속성은 양자역학에서의 기본적인 구성체가 양자라고 부르는 알갱이이기 때문에 발생한다. 가령 에너지의 예를 든다면 고전적으로 에너지는 연속된 임의의 값을 갖지만, 양자역학에서의 에너지는 모두 기본에너지 $\varepsilon = h\nu$ 의 정수배이다(h 는 프랑크 상수, ν 는 진동수). 따라서 임의의 에너지 값을 가질 수 없으므로 에너지 값은 불연속적이다. 원자 등의

* 고려대학교 정보보호대학원 ({hylee, quantum}@cist.korea.ac.kr)
** 고려대학교 정보보호대학원 부교수 (yangh@korea.ac.kr)

에너지 준위, 각운동량, 스핀도 마찬가지로 불연속적인 값만을 갖는다. 만약, 어떤 양자역학계가 불연속적인 두 상태로 이루어져 있는 것이라면 이진법의 0과 1을 나타내는 데 사용될 수 있게 된다. 위와 아래의 두 양자역학적 상태만이 가능한 스핀은 그 좋은 예가 된다.

현재 컴퓨터에서 사용되는 정보의 최소 단위인 비트(bit)에 해당하는, 양자 컴퓨터에서의 정보의 최소 단위를 양자 비트(quantum bit) 또는 큐빗(qubit)이라고 한다. 큐빗의 특징은 0 또는 1의 두 가지 값을 가질 수 있을 뿐 아니라 0과 1의 중첩 상태일 수 있다는 것이다. 양자 역학의 언어로 다시 말하면, 큐빗이란 위에서 설명한 불연속적인 두 양자역학계를 표시하는 $\{|0\rangle, |1\rangle\}$를 직교 기저(orthonormal basis)로 하는 2차원 Hilbert 공간에서의 임의의 상태를 의미한다. 따라서 큐빗의 일반적인 상태는 $a|0\rangle + b|1\rangle$로 표현되며, 여기서 a, b는 $|a|^2 + |b|^2 = 1$인 관계를 만족하는 복소수이다. 이때 $|a|^2$과 $|b|^2$은 각각 0과 1이 측정될 확률이다.

양자계산에서의 정보의 기본 단위 큐빗(qubit)은 일반적으로 중첩상태 $a|0\rangle + b|1\rangle$에 있게 된다. 양자계산에서는 이 중첩 상태에 대하여 양자역학적 상호작용을 가하여 연산을 수행한다. 따라서 고전적 연산은 0 아니면 1 에 대한 것이지만 양자계산은 무한히 가능한 여러 상태에 대한 연산일 수 있으며, 이를 적절히 이용하면 한 번의 연산으로 여러 계산을 동시에 수행하는 효과를 얻을 수 있다. 이를 양자병렬(quantum parallelism) 이라고 한다.

일반적인 양자상태인 중첩상태에 대하여 측정을 하면, 측정의 결과는 고유치 중의 하나로 나타난다. 고유치가 0과 1이라면, 측정 이전에는 중첩상태 $a|0\rangle + b|1\rangle$에 있었다고 하더라도 이에 대한 측정 결과는 고유치 중의 하나인 0 혹은 1이 된다. 더구나 측정 이후의 양자상태는 측정 결과의 고유치에 대응되는 상태인 $|0\rangle$이나 $|1\rangle$로 변하게 된다. 이처럼 측정 전의 양자 중첩 상태가 측정에 의하여 고유치에 대응하는 고유상태로 급격히 변하는 것을 측정에 의한 양자상태의 붕괴라고 한다.

불확정성의 원리 역시 측정과 관련되어 있다. 양자역학에서 모든 관측 가능한 물리량은 수학적으로 Hermitian 연산자로 표시된다. 측정하려는 물리량이 두 개 있다고 할 때, 만약 이 두 물리량에 대응되는 연산자가 교환되지 않는다면 이 두 물리량의 측정치에는 반드시 불확정성이 개입되며, 각 물리량의 불확정성의 곱은 어떤 상수 이상이라는 것이 불확정성의 원리이다. 한 예로 두 연산자 A 와 B 가 교환되지 않는다고 하자. 어떤 상태에 대해 연산자 A 로 측정을 하게되면 계의 상태는 A 의 고유치 중의 하나로 변한다. 그러나 그 다음에 연산자 B 로 측정을 하면 계는 다시 B 의 고유치 중의 하나로 변하게 되므로 바로 전의 상태에 대한 정보는 없어지게 된다. 이러한 현상은 양자암호에서 키를 교환하는데 이용될 수 있다.

고전 역학에서 볼 수 없는 특이한 양자현상의 하나가 얽힘(entanglement)이다. 두 입자로 이루어진 2 큐빗의 복합계의 경우, 그 양자상태가 개별계를 나타내는 양자상태의 텐서곱으로 표현되지 않게 되면 두 입자의 상태는 서로 강한 상관관계를 갖게 되는데 이러한 복합계의 양자상태를 얽힌 상태라고 한다. 이러한 얽힘은 하나의 큐빗을 교환함으로써 2 비트의 고전 정보를 전달하는 데에 사용될 수 있는데 이를 superdense coding 이라 부른다.

또 두 사람이 EPR 쌍을 미리 공유하고 있고 그 중 어느 한 사람이 어떤 양자상태 $|\phi\rangle$를 가지고 있다면, 이 $|\phi\rangle$에 대해 측정을 하지 않고도 고전적 통로를 통하여 다른 사람에게 이 $|\phi\rangle$의 상태를 전송할 수 있는데, 이를 양자원격전송(quantum teleportation)이라 한다. 이러한 얽힌 상태의 변환에 대한 여러 형태는 잡음이 있는 양자채널의 속성과 밀접한 관계를 갖기 때문에, 얽힌 상태는 양자정보이론의 중요한 도구로 이용된다.

광자의 편광(polarization) 방향은 원하는 방향으로 조정될 수 있다. 일반적으로, 빛은 여러 방향으로 편광된 광자로 구성되어 있다. 광자를 편광판에 통과시키면 특정한 진동 방향의 광자만이 투과되며 그 이외의 광자는 투과되지 않는다. 따라서 편광판을 이용하면 원하는 방향으로 편광된 빛을 만들 수 있다.

어떤 특정한 방향으로 편광된 광자가 편광판과 θ의 각을 이루면, 이 광자가 편광판을 통과할 확률은 $\cos^2\theta$이고, 편광판을 통과하지 못할 확률은 $1-\cos^2\theta$가 된다[1]. 편광과 불확정성과의 관계를 살펴보기 위하여, 십자형 편광은 수직 또는 수평으로 선형편광되어 입사하는 빛이고, 대각형 편광은 수평면과 45° 또는 135° 로 선형편광 되어 입사하는 빛이라고 하자.

수평과 수직 방향으로 편광된 상태를 각각 $|0^\circ\rangle$와 $|90^\circ\rangle$ 혹은 $\begin{pmatrix}1\\0\end{pmatrix}$과 $\begin{pmatrix}0\\1\end{pmatrix}$로 표현하자. 그러면 45°나 135°로 편광된 광자는 $|0^\circ\rangle$와 $|90^\circ\rangle$의 선형결합으로 다음과 같이 표현된다.

$$|45^\circ\rangle = \frac{1}{\sqrt{2}}\left(\begin{pmatrix}1\\0\end{pmatrix}+\begin{pmatrix}0\\1\end{pmatrix}\right)$$
$$= \frac{1}{\sqrt{2}}(|0^\circ\rangle + |90^\circ\rangle)$$
$$|135^\circ\rangle = \frac{1}{\sqrt{2}}\left(-\begin{pmatrix}1\\0\end{pmatrix}+\begin{pmatrix}0\\1\end{pmatrix}\right)$$
$$= \frac{1}{\sqrt{2}}(-|0^\circ\rangle + |90^\circ\rangle)$$

또, 역으로 $|0^\circ\rangle$와 $|90^\circ\rangle$의 상태는 $|45^\circ\rangle$와 $|135^\circ\rangle$의 선형결합으로 표시된다.

$$|0^\circ\rangle = \frac{1}{\sqrt{2}}(|45^\circ\rangle - |135^\circ\rangle) \quad (*)$$
$$|90^\circ\rangle = \frac{1}{\sqrt{2}}(|45^\circ\rangle + |135^\circ\rangle)$$

$|0^\circ\rangle$이 식(*)을 만족하므로 $|0^\circ\rangle$의 광자를 대각형 편광판으로 측정하면 45° 또는 135°로 편광된 빛이 각각 $\frac{1}{2}$의 확률로 측정된다. 측정 후의 상태는 $|45^\circ\rangle$혹은 $|135^\circ\rangle$인데, 이는 $|0^\circ\rangle$와 $|90^\circ\rangle$의 선형결합이다. 그러므로 이 광자를 십자형 편광판으로 측정할 때 0° 또는 90°로 측정될 확률은 각각 $\frac{1}{2}$이 된다.

이는 십자형 편광판과 관련된 정보를 완전히 소실하였다는 것을 의미한다. 이 예에서 보듯이 어느 한 광자에 대해 두 가지의 편광 상태가 동시에 부과될 수는 없다. 이러한 성질이 양자 키 분배 프로토콜에 이용된다.

Ⅲ. 양자 키 분배 프로토콜

사전에 어떤 비밀 정보도 갖고 있지 않은 두 사용자 갑과 을이 다른 이의 도청이나 변조가 없이 키를 공유하려는 것이 키분배이다. 고전 암호체계에서는 항상 수동적인 도청이 가능하기 때문에, 갑과 을이 도청이 발생했는지 여부를 모르는 채 비밀 정보를 전송하게 된다. 그러나 양자 암호체계에서는 앞 절에서 설명한 불확정성의 원리와 편광 등의 고유한 특성을 통하여, 전송되는 정보가 제 삼자에 의해 도청되거나 변조되었는지를 확인할 수 있어 안전한 키 분배가 가능해진다. 이러한 키분배 방식에서 양자 정보의 전송은 메시지를 직접 전달하는데 사용되기보다는 충분한 임의의 비트(random bit)를 전달하여 키를 공유하게 하는 데에 쓰인다. 이렇게 공유된 키는 one time pad의 키로 사용된다.[4]

1. BB84 프로토콜

먼저 1984년 Bennet과 Brassard에 의하여 처음으로 제시된 양자 키분배 프로토콜[5]에 대해 살펴보도록 하자. 이 프로토콜은 불확정성 원리를 기반으로 한 시스템인데, 흔히 BB84 프로토콜이라고 부른다. 앞으로 갑과 을은 사전에 비밀 정보를 갖고 있지 않은 사용자로 가정한다.

※ BB84 프로토콜의 과정은 다음과 같다.

1) 갑이 임의의 비트 수열(0과 1로 구성된 수열)을 선택하고, 각각의 비트를 편광 시킬 편광판(십자형 혹은 대각형)을 무작위로 선택한다.
2) 각각의 비트를 편광판으로 편광시켜 을에게 전달한다. 비트가 0인 경우 십자형 편광판에서는 ―로 편광시키고, 대각형 편광판에서는 ／로 편광시킨다. 비트가 1인 경우 십자형 편광판에서는 |로, 대각형 편광판에서는 ＼로 편광시킨다.
3) 을은 무작위로 선택된 편광판을 이용하여 전송되는 광자를 측정한다. 즉, 전송되는 각 비트마다 십자형 편광판과 대각형 편광판을 임의로 바꿔가며 측정한다.

이 단계까지가 양자 정보의 전송이다. 이렇게 전송이 완료되면, 갑과 을은 공개적으로 다음과 같은 과정을 수행한다. 아래에 소개되는 내용은 같은 비트를 공유하기 위하여 그렇지 못한 비트들을 제거하는 과정이라고 할 수 있다.

4) 을은 측정에 이용한 편광판의 순서를 갑에게 알려준다.
5) 갑은 4)의 편광판 중 자신이 사용한 편광판과 같은 편광판을 을에게 알려준다.
6) 같은 편광판을 사용한 정보만을 모은다.

도청이 없이 이 단계까지 수행되면 갑과 을은 같은 비트의 수열을 공유하게 된다. 도청이 없었다면 이 비트의 수열을 그대로 키로 사용해도 무방하지만, 도청이 발생할 수 있기 때문에 추가적으로 다음과 같은 과정을 수행하여 도청의 여부를 확인한다.

7) 을이 6)의 단계에서 모은 수열 중의 일부를 공개한다.
8) 갑은 7)의 정보를 확인한다.
9) 을이 7)에서 공개한 비트의 수열이 갑이 전송한 비트의 수열과 정확히 일치하면 이는 중간에 도청이 없었다는 것을 의미하므로 7)에서 공개하지 않은 정보를 그대로 비밀키로 사용하면 된다. 만일 두 비트의 수열이 정확히 일치하지 않는다면 이는 도청이 있었던 것이므로 교환된 비트의 수열을 전부 버리고 다시 위의 과정을 반복하여 키를 분배한다.

BB84 프로토콜에서 1 비트를 전송할 때 나타날 수 있는 모든 상황을 표로 정리하면 다음과 같다. 아래 표는 갑이 0과 1을 십자형이나 대각형 편광판을 사용하여 편광시킨 경우 각각에 대해 을의 측정 결과를 나타낸다. 같은 편광판을 사용했을 경우에는 확률 1로 갑과 같은 비트를 얻게되고, 다른 편광판을 사용했을 경우에는 확률 1/2로 같은 결과 값을 얻게 된다.

〔표 1〕 갑과 을 사이에 도청자가 없을 경우의 8가지 서로 다른 상황

갑이 보내려는 비트	갑이 사용하는 편광판	갑에서 을로 전송되는 광자	을이 사용하는 편광판	을이 측정하는 편광방향	을이 추정하는 비트
0	+	—	+	—	0
0	+	—	×	／ or ＼	0 or 1
0	×	／	+	— or |	0 or 1
0	×	／	×	／	0
1	+	|	+	|	1
1	+	|	×	／ or ＼	0 or 1
1	×	＼	+	— or |	0 or 1
1	×	＼	×	＼	1

시뮬레이터 안에 병이라는 도청자가 있을 경우를 살펴보자. 예를 들어 도청자 병이 있고, 갑은 0을 수직 편광판을 이용하여 을에게 보내는 경우를 생각하자. 병은 갑의 광자를 도중에 가로채어 그 편광방향을 측정한다. 그리고 자신의 도청 사실을 감추기 위해 자신이 측정한 광자를 을에게 전송한다. 을은 실제로 병에게서 오는 광자를 수신하지만 이 단계에서 자신이 수신하는 광자가 병에게서 오는 것인지를 확인할 수 있는 방법은 없다. 따라서 갑과 을은 프로토콜의 (1)~(3) 단계에서는 도청의 여부를 확인할 수 없다. 도청의 여부를 확인하기 위해서는 프로토콜의 (4)~(6) 단계를 거쳐 (7)~(9)의 단계를 수행하여야 한다.

〔표 2〕 갑과 을 사이에 도청자 병이 있을 경우의 16가지 서로 다른 상황

갑이 보내려는 비트	갑이 사용하는 편광판	갑에서 병으로 전송되는 광자	병이 사용하는 편광판	병에서 을로 전송되는 광자	을이 사용하는 편광판	을이 측정하는 편광방향	을이 추정하는 비트
0	+	—	+	—	+	—	0
0	+	—	+	—	×	／or＼	0or1
0	+	—	×	／or＼	+	—or |	0or1
0	+	—	×	／or＼	×	／or＼	0or1
0	×	／	+	—or |	+	—or |	0or1
0	×	／	+	—or |	×	／or＼	0or1
0	×	／	×	／	+	—or |	0or1
0	×	／	×	／	×	／	0
1	+	|	+	|	+	|	1
1	+	|	+	|	×	／or＼	0or1
1	+	|	×	／or＼	+	—or |	0or1
1	+	|	×	／or＼	×	／or＼	0or1
1	×	＼	+	—or |	+	—or |	0or1
1	×	＼	+	—or |	×	／or＼	0or1
1	×	＼	×	＼	+	—or |	0or1
1	×	＼	×	＼	×	＼	1

도청자(병)가 채널에 존재하여 도청을 시도할 때 나타날 수 있는 상황을 표로 정리하면 위의 〈표 2〉와 같다. 이 표를 보면, 갑, 을, 병이 모두 같은 편광판을 사용했을 경우에는 도청을 확인할 수 없다. 그런데 BB84 프로토콜에서 도청을 확인하는 작업은 갑과 을이 같은 편광판을 사용했을 경우에 측정된 비트만을 확인하는 것이므로, 갑과 을이 같은 편광판을 사용하고 병이 다른 편광판을 사용하는 경우에만 1/2의 확률로 도청의 확인이 가능하다. 그러므로 도청이 있었음에도 불구하고 도청이 확인되지 않을 확률은 3/4 이다. 도청확인을 위하여 n개의 비

트를 사용한다면, 도청을 확인할 수 있는 확률은 $1-\frac{3}{4}^{n}$이다. 따라서 n을 충분히 크게 하면, 위의 양자 키 분배 프로토콜은 거의 완벽하게 도청 여부를 확인할 수 있어 안전한 키분배를 가능하게 한다. 지금까지 설명한 BB84 프로토콜이 양자 키분배 프로토콜 중 제일 처음 제안된 것이지만, 이후로 제안된 여러 양자 키 분배 프로토콜들은 이와 유사한 체계를 따르고 있다.

2. EPR 프로토콜

다음으로 EPR 쌍을 이용하는 EPR 프로토콜[7]을 살펴보자. EPR 프로토콜은 갑에 의해 키가 생성되는 BB84 프로토콜과는 달리, 얽힘(entanglement)의 성질을 이용하여 원칙적으로 무작위적인 키가 생성된다. 즉, 누군가의 의도대로 키가 생성되는 것이 아니라 키를 생성하는 사람도 어떤 키가 생성될 지 모르는 무작위성이 나타난다.

EPR 프로토콜에 사용되는 채널은 EPR상태를 방출할 수 있는 장치로 구성되어있다. 채널에서 방출된 광자는 합법적인 사용자 갑, 을에게 한쪽씩 전달된다. 갑과 을은 각각 이 광자를 세 방향중 한 방향으로 측정하여 저장한다.

만약 갑이 $\phi_1=0,\ \phi_2=\frac{1}{4}\pi,\ \phi_3=\frac{1}{2}\pi$ 방향을 택하고, 을이 $\psi_1=\frac{1}{4}\pi$, $\psi_2=\frac{1}{2}\pi$, $\psi_3=\frac{3}{4}\pi$ 방향을 택한다고 하자. 그러면 갑과 을의 측정에 대한 상호 정보의 양은 다음과 같이 주어진다

$$E(a_i, b_j)=P_{++}(a_i, b_j)+P_{--}(a_i, b_j) \\ -P_{+-}(a_i, b_j)-P_{-+}(a_i, b_j)$$

$P_{\pm\pm}(a_i, b_j)$는 a_i로 측정했을 때의 결과가 $\pm$이고, b_j로 측정했을 때의 결과가 $\pm$인 경우의 확률을 나타낸다. 따라서 $E(a_i, b_j)=-a_i\cdot b_j$ 라고 할 수 있다.

위의 경우에서 $\phi_2=\psi_1$이고 $\phi_3=\psi_2$이기 때문에 $E(a_2, b_1)=E(a_3, b_2)=-1$이 된다. 따라서 다른 방향의 편광판을 사용한 갑과 을의 상호 정보의 양 S는 다음의 식[6]으로 정의되고 그 값은 $-2\sqrt{2}$이 된다.

$$S=E(a_1, b_1)-E(a_1, b_3)+E(a_3, b_1)+E(a_3, b_3)$$

전송이 끝난 뒤에 갑과 을은 각각의 비트를 측정하는데 사용한 편광판의 방향을 공개하고, 같은 편광판을 사용하였는지의 여부에 따라 측정 비트를 두 그룹으로 분류한다. 한 그룹을 서로 다른 방향의 편광판을 사용한 비트들의 집합이고, 다른 그룹은 같은 방향의 편광판을 사용한 비트들의 집합이다. 도청이 없을 경우, 이 두 번째 그룹이 키의 역할을 하게 된다.

도청을 확인하기 위하여 첫 번째 그룹, 즉 다른 편광판을 사용한 비트들에 대해 S값을 계산한다. 도청이 발생한 경우에 S는 -1과 1사이의 값이 되는데, 이는 절대로 앞에서 제시한 $-2\sqrt{2}$값이 되지 않기 때문에 도청을 확인 할 수 있다.

※ EPR 프로토콜을 정리하면 다음과 같다.

0) 사전단계로 EPR 상태를 전송할 수 있는 채널을 설정한다.
1) EPR 수열을 갑과 을에게 전송한다.
2) 갑과 을은 각자의 편광판의 방향을 바꿔가면서 측정한다.
3) 편광판 방향을 공개한다.
4) 편광판의 동일성 여부에 따라 측정된 수열을 분류한다.
5) 다른 편광판을 사용하여 측정된 비트들을 공개한다.
6) 상호 정보의 양 S를 계산하여 특정한 값이 나오면 같은 편광판을 사용하여 측정된 수열을 키로 선택하고, 그렇지 않으면 다시 키분배를 실시한다.

EPR 프로토콜의 특징은 BB84 프로토콜에서 쓸모 없이 버렸던 비트들을 이용하여 도청의 여부를 확인할 수 있다는 점이다. 키분배를 위하여 BB84 프로토콜에서는 원하는 키 길이의 4배정도의 무작위적인 비트를 전송해야하는 데 반하여, EPR 프로토콜에서는 그것의 반정도만 전송하면 되기 때문에 전송비용이 BB84보다는 적게 들고 더 빠르게 비트들을 전송할 수 있다. 그러나 한편 갑과 을이 각각 S를 계산해야 하므로 약간의 번거로움이 있을 수 있다.

3. 그 밖의 양자 키 분배 프로토콜

앞에서 제시된 BB84 프로토콜과 EPR 프로토콜은 채널에서 발생할 수 있는 오류의 영향을 고려하

지 않고 있다. 따라서 실제로 사용되기 위해서는 채널 상에 발생하는 오류를 복구하는 과정이 필요하다. 이러한 목적으로 제안된 대표적인 프로토콜에는 Lo와 Chau의 프로토콜[8](간단히 modified Lo-Chau 프로토콜이라고 부른다)과, 이 프로토콜에 CSS 코드를 적용시킨 키분배 프로토콜[3], 그리고 BB84 프로토콜을 변형시킨 일명 Secure BB84[9] 프로토콜 등이 있다.

Modified Lo-Chau 프로토콜은 EPR 프로토콜과 같이 EPR 쌍을 사용하고, 오류를 복구하기 위하여 t개까지의 오류를 복구할 수 있는 [n,m]양자 코드를 사용한다. 이에 반하여 CSS 코드를 사용한 양자 키분배 프로토콜은 이름에서 드러나는 것처럼, modified Lo-Chau프로토콜에서 [n,m]양자 코드 대신에 CSS 코드를 사용하였다. 마지막으로 Secure BB84 프로토콜은 BB84 프로토콜에 CSS 코드를 적용시켜 안전하고 정확한 키 분배가 이루어지도록 고안되었다.

이상에서 논의한 양자 키 분배 프로토콜의 내용을 정리하면 다음과 같다. 지금까지 제안된 양자 키 분배 프로토콜은 BB84에서 시작된다. 이 프로토콜을 개선하여 버리는 비트들까지 이용하도록 고안된 것이 EPR 프로토콜이다. 이 두 프로토콜을 통하여 원칙적으로 거의 완벽하게 안전한 키 분배가 이루어지기는 하지만 실제 적용의 문제가 있기 때문에, 이후 제안된 프로토콜들은 오류수정과 같은 작업들이 추가되었다.

Ⅳ. 결 론

지금까지 양자 키 분배 프로토콜에 대해 간단히 살펴보았다. 양자역학의 원리를 이용한 Shor의 알고리즘이 현존하는 공개키 암호 시스템을 공격할 수 있는 방법을 제시한다고 하면, 같은 양자역학의 원리를 이용한 양자 키분배 프로토콜은 거의 완벽하게 안전한 키를 분배하는 방법을 제시해 준다. 그리고 이러한 양자 암호 분야는 이미 어느 수준 이상의 구현에 성공하였고 계속 개발 중에 있다. 우리나라에서는 양자 암호분야에 대한 연구가 시작된 지 얼마 되지 않았지만 앞으로 지속적인 관심과 연구 활동이 이루어져야 할 것이다.

참고문헌

[1] C. P. Williams, S.H. Clearwater, "Explorations in Quantum computing"

[2] R. Shankar, "Principles of Quantum Mechanics", pp.245-247

[3] A. Nielsen and L. Chuang, "Quantum information and Quantum information", CAMBRIDGE UNIVERSITY PRESS

[4] Charles H.Benett, Francois Bessette, Gilles Brassard, "Experimental Quantum Bryptography", cryptology5:3-28, 1992

[5] Charlse H.Bennett and Gilles Brassard, "Quantum Cryptography : Public key distribution and coin tossing" in proceeding of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India 1984, (IEEE Press, 1984)

[6] Alain Aspect, Philippe Grangier and Gerard Roger, "Experimental Realization of Einstein - Podolsky - Rosen - Bohm Gedankenexperiment : A New Violation of Bell's Inequalities", Phys.Rev.Lett., 49(2): 91-94, 1982

[7] Artur K.Ekert, "Quantum Cryptography Based on Bell's theorem "Phys.Rev. Lett., 67(6):661-663, 1991

[8] Hoi-Kwong Lo and H.F.Chau, "Unconditional Security of Quantum key distribution over arbitrarily long distances" SCIENCE vol 283, 2050-2056, 1999

[9] Peter W.Shor and John Preskill, "Simple Proof of Security of the BB84 Quantum Key Distribution Protocol", arXiv : quant-ph/003004 v2, 2001

〈著者紹介〉

이 화 연 (Hwa-Yean Lee)

2001년 2월 : 고려대학교 이과대학 수학과 졸업

2002년 3월~현재 : 고려대학교 정보보호대학원 정보보호학과 석사과정

관심분야 : 양자암호, CMVP, 암호프로토콜

조 규 형 (Kyu-Hyung Cho)

2001년 2월 : 서울시립대 수학과 졸업

2001년 3월~현재 : 고려대학교 정보보호대학원 정보보호학과 석사과정

관심분야 : 양자 암호, 암호프로토콜

양 형 진 (Hyungjin Yang)

정회원

1990년 8월~1990년 10월 : 미국 Oak Ridge 국립연구소, Computer Consultant.

1990년 12월~1991년 12월 : 미국 신시내티대학교 박사후 연구원.

1999년 1월~1999년 12월 : 미국 매릴랜드대학교 교환교수.

1992년 3월~현재 : 고려대학교 자연과학대학 물리학과 교수.

2001년 3월~현재 : 고려대학교 정보보호대학원 겸임교수.

관심분야 : 양자암호, 암호프로토콜