양자 암호의 보안성 재고와 프로토콜 개선을 통한 보안성 향상

배준우
한양대학교

요 약

양자 통신에서 양자 채널은 일반적으로 잡음을 수반하여 송신자가 보낸 양자 신호들에 잡음을 더하고 신호의 왜곡을 생성하는데, 일반적으로 이 잡음의 정도는 송수신자 간의 통신을 통해 규명할 수 있다. 본 논문에서는 양자 암호 프로토콜에서 양자 채널의 구성에 고차원의 양자계가 적용되었을 때 보안성을 얻을 수 있는 양자 채널의 조건들을 살펴보고자 한다. 특별히 고차원의 양자 신호를 사용하고 양방향 통신을 활용하여 안전한 양자 암호 프로토콜이 견딜 수 있는 한계 잡음 수준을 올릴 수 있음을 보이고자 한다. 본 연구의 결과는 2차원의 양자 신호를 사용하는 양자 암호 프로토콜인 Bennett-Brassard-1984 프로토콜, six-state 프로토콜 등에 적용할 수 있으며, 확장된 일반적인 d차원에서 2-기저 프로토콜 혹은 (d+1)-기저 프로토콜 등에 적용할 수 있다.

Ⅰ. 서 론

통신이 정보의 양적인 부분을 평가한다면 암호는 정보의 질적 수준을 평가한다. 암호는 보안성을 지닌 정보와 보안성을 지니지 않은 정보를 구별한다. 현대 암호는 보안성의 개념을 구체화하여 보안성을 수학적 형식으로서 정의하기 시작했다. 이는 현대 암호의 가장 큰 기여 중 하나로 꼽힌다.

암호의 현대적 접근에서 특정 암호 장치의 보안성의 판별을 위한 첫 번째 과정은 보안성이란 무엇을 의미하는지 수학적으로 정확히 정의 하는 것이다. 두 번째는 그러한 정의는 어떠한 가정 하에서 유효할 수 있는지를 밝히는 것이다. 마지막으로, 그러한 가정 하에서, 구현된 특정 암호 장치가 앞서 명시한 암호의 보안성 정의로 환원되는지 혹은 환원되지 않는지를 판별하는 것이다. 만일 환원된다면, 보안성의 충분 조건을 만족함을 보였다고 할 수 있다. 이를 보안성 조건이라고 부르며, 대응하는 암호 장치의 프로토콜은 증명가능한 보안성을 지니고 있다고 한다. 환원되지 않음을 보였다면, 즉 환원을 위한 필요조건들을 만족하지 않음을 보였다면, 비보안성 조건이라고 한다. 흥미롭게도, 암호에서 가정과 보안성은 서로 상보적인 관계를 지니고 있다. 많은 수의 가정들 하에서 얻은 보안성은 적은 가정들 하에서 얻은 보안성보다 낮은 수준의 보안성이다.

암호 수행의 재료가 되는 정보는 그 자체로 정의하기 난해한 개념이다. 그 어려움은 물리학에서, 가령 에너지와 같은, 고유 양들을 직접 정의하기 까다로운 그것과 유사하다. 실제로 정보와 물리는 밀접한 관계를 지니며 그 관계들을 여러 각도에서 분석하기도 한다. 부정할 수 없는 사실은, 물리 법칙이라는 지배하에서 물리계는 정보 전달을 수행하고 정보 처리 역시 이러한 물리 법칙의 영역 안에서 정량화될 수 있으며 한계점을 지닌다는 것이다. 가령, 1 비트에 해당하는 정보의 송신은 어느 수신자에게도 1 비트 이상의 정보양의 수신을 허용하지 않는다. 이는 물리학의 인과율을 정보 처리에 대응하여 얻는 결과이다.

정보 처리를 수행할 수 있는 물리 시스템의 근본 단위는 전자기 시스템을 뛰어넘어 원자, 광자, 전자 등과 같은 양자 시스템들이다. 양자 시스템들은 양자 이론의 공리들을 따르며 양자 공리들은 고전 물리학의 원리들과는 – 다른 물리 이론들은 서로 일관성 있게 설명될 수 있으나 – 원칙적으로 독립적이다. 다시 말하면, 전자기학 단위에서의 정보 처리는 그 근본 단위인 양자 시스템에서의 정보 처리와 매우 상이하다. 더 작은 물리 시스템에서의 정보 처리로서 비교하는 것 이상으로, 다른 물리법칙 – 전자기학과 양자이론 – 의 적용을 받는 정보 처리의 다른 패러다임으로 고려하는 것이 적절하다. 양자 정보 이론은 정보이론과 원칙적으로 구별되며 그러한 성질들은 양자 암호 프로토콜의 작동 원리 및 보안성 원리의 근간이 된다.

양자 정보 이론에서는 정보 처리의 비트개념을 확장하여 양자 정보의 단위인 양자 비트를 사용하고 큐빗 (Qubit)이라 부르며, 정보 이론의 d 값 분포를 지닌 시스템들은 큐딧 (Qudit) 으로 대응된다. 양자 정보 이론이 정보 이론과 구별되는 특징 중 하나는 바로 상관관계이다. 정보 이론에서 시스템들 간의 확률 분포, 혹은 이를 이용한 공유 정보 등으로 표현되는 상관관계는 양자 얽힘 (Entanglement) 으로 표현되는 양자 상관관계

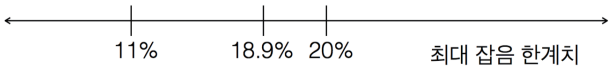
를 표현해 낼 수 없다. 이러한 양자 얽힘은 양자 통신과 양자 시스템들의 많은 성질들을 포괄하고 있다. 예를 들어, 양자 얽힘은 양자 상태의 일반적인 공유 불가능성을 포함하고 있으며 또한 복제 불가능성과 양자 상태들의 100%상태 구별의 불가능성 등을 포함하고 있다. 앞서 언급한, 공유 불가능성, 비복제성, 100% 상태 구별 불가능성 등은 통신에서 전자기 시스템이 포함하는 정보에 대한 양자 시스템이 포함하는 정보의 질적인 구별을 의미한다. 특별히, 이러한 성질들은 보안성을 지닌 정보가 지닌 성질들과도 일치한다 – 암호화된 정보는 공유되어서도 안 되고, 타인에게 복제되어 분배되어서도 안 되며, 마치 난수와 같이, 100% 구별되는 신호여서도 안 된다. 즉, 양자 정보는 보안성을 지닌 정보로 자연스럽게 환원될 수 있는 가능성을 내포한다. 실제로 최대로 얽힌 양자 상태 (maximally entangled state) 의 검증은 양자 암호의 보안성의 정의이다.

여기서 보안성은 대칭키 암호 혹은 비밀키 암호의 보안성을 의미하며, 이는 20세기 중반 섀논 (C. Shannon) 에 의해 정보이론의 방법으로 증명된 보안성이다. 따라서, 양자 암호의 보안성의 정의는 최대 얽힘의 검증이며 – 혹은 최대 양자 얽힘의 검증으로 환원가능– 이 보안성은 정보 이론을 바탕으로 증명 가능한 보안성이다. 양자 암호 프로토콜은 양자 물리학이 양자계를 옳게 기술하는 이론이라는 물리법칙을 가정하고 있다. 양자 암호 프로토콜은 가장 적은 가정들에 해당되며 따라서 가장 높은 수준의 보안성을 포함한다.

반면, 현대 암호의 보안성은 계산 복잡도 이론에 기반을 둔 계산 보안성을 의미하며, 증명되지 않은 계산 복잡도에 근거하고 있다. 실제로 계산 복잡도의 대부분은 가설로 남아 있는 난제들이며 이로 인하여 보안성과 비보안성을 정확히 판별하기 난해하다. 한편, 1990년 대 중반 양자 소인수 분해 알고리즘은 현대 암호는 양자 전산이라는 미래 기술에 대해서는 더 이상 안전하지 않음을 명쾌히 보였다.

양자 암호 프로토콜이 원리적으로 보안성을 지닐 수 있음은 2000년 쇼어(Shor) 와 프레스킬(Preskill)에 의해 보여졌다 [1]. 최초 양자 암호 프로토콜인 Bennett–Brassard–1984 (BB84) 프로토콜이 1984년도에 개발된 후에, 1990년대 양자 소인수 분해 알고리즘의 개발을 통하여 RSA 암호와 같은 현대 암호의 비대칭 암호의 보안성이 시한부라는 과정을 거치며, 2000년도에 와서야 양자 암호의 보안성이 실용적 가치를 인정받으며 주목받게 되었다. 초기 증명에서는, 양자 통신의 두 주체인 갑과 을이 신뢰할 만한 안전한 측정 장치를 사용하고 난수 발생을 통한 신호 생성을 한다는 가정 하에서, 갑과 을을 연결하는 공유 양자 채널에 잡음이 있는 경우를 고려하였다. 잡음의 한계가 0%라면 완벽한 보안성을 의미한다. 2000년도 쇼어와 프레스킬의 증명은 잡음의 정도가 11% 미만이라면, 단방향 오류 정정 코드 등을 사용하여 보안성을 지닌 비밀키를 얻을 수 있음을 보였다. 이 때 채널 잡음이 11% 미만이라면, 채널에 대한 어떠한 공격에도 안전함을 의미한다.

11%의 잡음 한계는 일반적으로 광케이블의 성질을 고려할 때 구현 가능한 한계치로 고려될 수 있으나, 실제로 장거리 통신 등의 실용적인 통신에서는 이 한계치를 쉽게 초과하여 안전한 암호의 구현은 어려울 수 있다. 이러한 구현의 문제를 극복하는 프로토콜을 개발하고자 양방향 오류 정정부호, 양자 통신의 일반화 과정 등이 고려되었는데, 주목할 만한 결과는 2003년 고테스만 (Gottesman) 과 로(Lo) 에 의해 보여진 양방향 통신을 통한 오류 정정 부호의 활용이다 [2]. 일반적인 양방향 오류 정정 부호의 개발은 양자 정보 이론에서 매우 어려운 문제 중의 하나이므로, 고테스만 (Gottesman) 과 로(Lo)는 특정 양방향 통신을 적용하였고, 그 결과 BB84 프로토콜을 활용하는 경우 18.9%의 잡음까지 견딜 수 있는 양자 암호 프로토콜을 개발하였다. 이 결과는 초기의 쇼어와 프레스킬의 양자 오류 정정 부호를 양자 암호에 적용하는 방법을 양방향 통신으로 확장하여 임의의 큐빗 상태들에 적용할 수 있으나, 오류 정정 부호의 고차원 일반화의 어려움으로 인해 일반적인 큐딧에는 적용의 한계가 있다.



2007년 정보 이론의 접근을 적용하여 양방향 통신을 사용하는 양자 암호 프로토콜을 개선하고 보안성 조건들을 유도한 연구 결과가 발표되었다 [3]. 이 결과는 큐빗 뿐만 아니라 일반적인 고차원의 양자 시스템인 큐딧에도 적용할 수 있는 보안성 조건을 제시하였으며, 일반적인 잡음이 채널에 생기는 경우에도 적용가능하다. 개선된 프로토콜을 BB84 프로토콜에 적용하였을 때 양자 암호 프로토콜이 견딜 수 있는 최대 잡음 한계치는 20%로 개선되었다. 현재까지도 이 결과는 더 개선되지 않고 있다. 반면, 보안성을 위한 필요조건은 잡음 비율 25%로 알려져 있다. 따라서, 20%와 25%사이의 해당되는 양자 암호 프로토콜은 현재로서 그 보안성 판별이 되지 않는다.

본 논문에서는 고테스만 (Gottesman) 과 로(Lo) 타입의 양자 암호 프로토콜 보안성 분석을 재고하여 고테스만 (Gottesman) 과 로(Lo)의 보안성 조건을 2007년의 결과와 같이 향상하고자 한다. BB84 에 적용했을 때에는 18.9%의 한계 잡음을 20%까지 향상할 수 있음을 의미한다. 또한, 일반적인 고차원 양자 시스템인 큐딧에도 적용하여, 고차원 양자계를 양자 암호에 적용하였을 때 보안성 조건을 얻고자 한다.

Ⅱ. 본 론

본론에서는 양방향 양자 암호의 보안성 분석을 살펴보고자 한다. 먼저, 양자 암호의 재료가 되는 양자 얽힘을 소개하고, 양자 얽힘을 묽게 만드는 잡음이 과정을 역수행하는 양자 오류 정정 부호 및 동치 과정인 양자 얽힘 증류를 소개하고자 한다. 그리고 양자 암호의 보안성 분석과의 관계를 알아보고 양방향 양자 암호 프로토콜의 보안성 조건을 살펴본다.

1. 양자 얽힘, 양자 오류 정정 부호, 양자 얽힘 증류 및 양자 암호의 보안성

[1]에서 양자 암호 보안성 증명 방식은 양자 오류 정정 부호를 사용한다. 먼저 갑(A)이 다음과 같은 최대 얽힘 상태,

$$|\phi^+\rangle_{AB}^{\otimes N} \quad |\phi^+\rangle_{AB} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \qquad (1)$$

를 충분히 큰 N개 상태를 생성하고 반을 가진 후에 나머지 반을 을(B)에게 주었다고 하자. 이 때 을에게 줄 때에는 잡음이 섞이게 되는데 이는 갑이 잡음을 의도적으로 섞는 과정과 동일하다. 잡음의 정도가 너무 높지 않다면, 후에 갑과 을은 양자 오류 정정 부호를 사용하여 원래 상태인 최대 얽힘 상태를 환원할 수 있다. 논문 [1]에서는 먼저 그 잡음의 한계치를 보였으며, 그리고 양자 얽힘의 분배 및 증류 방식과 동치가 되는 실제 양자 암호 프로토콜에 해당되는 준비-및-측정 프로토콜이 존재함을 증명하였다. 가령 BB84 프로토콜은 그러한 준비-및-측정 프로토콜의 한 예가 된다. 따라서, [1] 논문에서의 증명은 일반적인 준비-및-측정 프로토콜의 보안성 분석에 유효하며, BB84 프로토콜에 적용되었을 때 11%의 한계치를 제공한다. 여기서 양자 오류 정정 부호는 특별히 Calderbank-Shor-Steane (CSS)코드를 활용하였는데 이는 단방향 양자 얽힘 증류과정과 동일하다.

논문 [2] 에서는 CSS 코드를 뛰어넘어 양방향 양자 오류 정정 부호를 적용하고자 하였다. 또한 양자 오류 정정 부호와 양자 얽힘 증류가 서로 동치라는 결과를 활용하였다. 따라서, 양방향 양자 얽힘 증류에 대응하는 양방향 양자 오류 정정 부호를 적용하여 최대 양자 얽힘을 얻을 수 있는 잡음의 한계치를 구할 수 있으며, 이 결과는 일반적인 준비-및-측정 프로토콜에 유효하여 양방향 통신을 포함하는 BB84 프로토콜 등에 적용될 수 있다.

실제로, 양방향 통신의 수학적 일반화는 매우 어려운 문제로 알려져 있다. 이는 양자 정보 이론 수준에서 일반적인 통신수반-국소연산 (Local Operations and Classical Communication, LOCC)의 일반적인 모델을 찾는 것과 동일하다. 따라서 양자 얽힘 증류의 일반적인 양방향 통신 모델을 제시하는 것 또한 난제로 고려된다. 통신 모델에서 1993년 Maurer가 제시한 특정-증류 (Advantage Distillation, AD) 프로토콜은 대칭 암호에서 비밀키 증류를 위한 잡음의 한계치를 매우 완화하였다[4]. 1998년 이 프로토콜은 양자 얽힘 증류에 적용되어, 양방향 양자 얽힘 증류 방법이 제시되었다[5]. 가장 일반적인 양방향 양자 얽힘 프로토콜이라고 할 수 있을지는 알려져 있지 않으나, 두 개의 큐빗 상태들의 경우, 이 프로토콜은 모든 얽힌 양자 상태들에 대해서 작동함이 보였다[5]. 즉, 양자 얽힘 증류 프로토콜 하에서, 양자 얽힘 증류 조건과 양자 얽힘의 조건이 일치한다 [5]. 따라서, 양방향 양자 얽힘 증류의 방법을 적용하여 양자 오류 정정 부호 활용을 기반으로 양방향 양자 암호 프로토콜의 보안성을 증명할 수 있다.

표 1. 양자 정보 이론과 정보 이론의 대응관계 [6]

양자 정보 이론	정보 이론
최대 양자 얽힘	비밀키
양자 얽힘 증류	키 증류 (키 생성)
양자 오류 정정 부호	선형 오류 정정 부호
양자 전송 (Quantum Teleportation)	원타임패드(One-time Pad)
통신수반-국소연산 Local Operations and Classical Communication (LOCC)	공공통신-국소연산 Local Operations and Public Communication (LOPC)

여기서 양자 암호의 보안성은 임의의 공격에 대해서 안전함을 의미한다. 일반적으로, 채널 공격은 채널을 개별로 공격하는, 가장 낮은 수준의, 개별 공격 (individual attack), 그리고 도청자의 양자 메모리를 활용한 집단공격(collective attacks), 마지막으로 가장 강력한 일반적인 공격인, 복합 공격 (coherent attacks)으로 분류할 수 있다. 예를 들어, 개별 양자 상태를 복제하여 공격하는 방법은 개별 공격의 한 종류이다. 집단 공격에서는 도청자는 양자 메모리를 활용하여 자신의 양자 시스템의 측정 시점을 임의대로 미룰 수 있다. 집단 공격은 특정한 경우 복합 공격만큼 강한 공격임이 알려져 있기도 하다. 본 논문에서는 가장 일반적이고 높은 수준의 보안성인 복합 공격에 대한 보안성을 논의한다.

2. 양방향 양자 암호의 보안성

지금부터는, 양방향 얽힘 증류 프로토콜을 적용하여 일반적인 d 차원이 양자 시스템을 양자 암호 프로토콜에 적용하였을 때 보안성의 조건을 구하고자 한다. 먼저, 식 (1) 에서의 큐빗의 경우를 일반화하여 d 차원의 최대 얽힘 상태는 다음과 같다:

$$|B_{0,0}\rangle = \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} |k\rangle|k\rangle \quad (2)$$

갑은 위의 상태를 충분히 큰 N에 대하여 N 쌍을 생성하여 반을 가진 후에 나머지 반을 을에게 전송한다. 전송 시에는 일반적인 잡음 모델 하에서 잡음이 섞이게 되어 갑과 을의 공유하는 양자 상태는 일반적으로 힐버트 공간에서 상한이 주어진 연산자로 다음과 같이 표현된다:

$$\rho_{AB}^{(\times N)} \in \mathcal{S}(\mathcal{H}_d^{\otimes N} \otimes \mathcal{H}_d^{\otimes N})$$

여기서 갑과 을의 2N개의 양자 시스템들은 모두 d차원의 힐버트 공간 상에 연산자로 표현된다. 그리고 갑과 을은 능동적으로 공유하는 쌍에 대해 바일 대칭 연산 (Weyl symmetrisation) 으로 불리는 다음과 같은 통신 수반-국소 연산 (LOCC) 을 수행할 수 있다:

$$\rho \to \sum_{m,n=0}^{d-1} U_{m,n} \otimes U_{m,n} \rho U_{m,n}^{\dagger} \otimes U_{m,n}^{\dagger} \quad (4)$$

여기서 유니타리 연산자들은 다음과 같이 정의된 바일 연산자들 (Weyl operators) 이고

$$U_{m,n} = \sum_{k=0}^{d-1} e^{-\frac{2\pi i}{d} kn} |k+m\rangle\langle k| \quad (5)$$

d차원 양자 상태들에 대해 비트 - 에러와 위상-에러의 생성을 표현한다. 또한 연산자 공간에서 기저이다. 최대 얽힘 상태가 임의의 바일 연산자로 표현되는 잡음의 영향을 받았을 때, 식 (5)의 바일 연산자의 표현을 이용하여 다음의 상태가 생성된다:

$$\begin{aligned} |B_{m,n}\rangle &= (id \otimes U_{m,n})|B_{0,0}\rangle \\ &= \frac{1}{\sqrt{d}} \sum_{k} e^{-\frac{2\pi i}{d} kn} |k\rangle|k+m\rangle \end{aligned} \quad (6)$$

식 (4)에 표현된 바일 대칭화 후에 갑과 을이 갖는 상태의 각 쌍은 다음의 혼합 상태로 표현된다.

$$\rho = \sum_{m,n=0}^{d-1} q_{mn} |B_{m,n}\rangle\langle B_{m,n}| \quad (7)$$

이는 식 (2)의 초기의 최대 얽힘 상태에 각각의 비트-에러와 위상-에러가 확률적으로 생성되어 식 (6)에 표현된 잡음 섞인 상태들이 혼합된 평균 상태로서 해석할 수도 있다.

오류 정정 부호 프로토콜은 위의 N쌍의 혼합 상태들에 존재하는 오류들을 수정하여 N보다 적은 수의 n개의 최대 얽힘 상태를 얻는다. 이는 양자 얽힘 증류와 동일한 과정이다. 여기서 사용된 양자 상태들의 개수에 대한 생성된 최대 얽힘 상태의 개수의 비율의 극한

$$Y = \lim_{N \to \infty} \frac{n}{N}$$

을 수율이라고 부르며, 양자 얽힘 증류의 효율성을 의미한다. 수율이 0보다 크다면, 양자 얽힘 증류 프로토콜이 작동하여 최종적으로 최대 양자 얽힘을 얻을 수 있음을 뜻한다. 수율이 0이라면 최대 양자 얽힘은 생성되지 않는다. 양자 얽힘 증류에 적용되는 초기 양자 상태가 양자 얽힘을 가지지 않은 분리 가능한 (separable) 상태라면 양자 얽힘 증류의 수율은 0이다. 여기서는 식 (7)의 양자 상태가 양자 얽힘을 포함하고 있을 때 수율이 0보다 클 가능성이 있다. 일반적으로 주어진 양자 상태들로부터 최대 양자 얽힘을 증류할 수 있는지 여부를 판별하는 문제는 난제로 알려져 있고, 이 경우에도 식 (7)에 나타난 상태들에 대해 양자 얽힘 증류의 가능성 판단은 알려져 있지 않다. 양자 얽힘 증류가 불가능한, 식 (7)의 상태에 대한, 얽힘 혹은 분리가능의 조건 또한 알려져 있지 않다. 식 (7)에 상태의 얽힘 조건에 대한 필요조건을 보였으나 일반적인 해법은 미해결로 남아있다.

수율을 직접 계산하는 일반적으로 어려운 일이며, 수율이 0보다 큰 지를 판별하는 것은 양자 얽힘 증류가 가능한 지를 판별하는 것이며, 즉 대응되는 오류 정정 부호 프로토콜이 작동하고, 결과적으로 대응되는 준비-및-측정 양자 암호 프로토콜이 보안성을 가질 수 있음을 의미한다.

양방향 양자 얽힘 증류 프로토콜은 다음과 같이 작동한다 [5]. N쌍의 첫 번째 두 쌍에 대해 얽힘 증류 프로토콜을 적용한 후에 두 번째 쌍을 측정하고 그 측정값이 같으면 첫 번째 쌍을 받아들이고 같지 않으면 첫 번째 쌍을 버린다. 측정값이 같은 경우는 확률적으로 발생한다. 다시 바일 대칭화를 적용하여 첫 번째 쌍을 식 (7)의 상태로 능동적으로 변환한다. 이제 세 번째 상을 도입하여, 바일 대칭화 후에 첫 번째 쌍과 함께 같은 과정을 반복하고, 역시 세 번째 쌍을 측정하여 측정값의 일치의 결과에 따라 확률적으로 첫 번째 쌍을 받아들인다. 계속 반복하는데, 측정값이 같은지를 확인하는 과정은 오류-정정 (error-correction) 에 해당하며, 능동적으로 식 (7)의 상태로 변화하는 바일 대칭화 과정은 비밀-증폭 (privacy amplification) 에 해당한다. 오류-정정과 비밀-증폭의 순서는 바뀔 수 있으며 그 순서에 따라 수율에는 변화를 줄 수 있으나 양자 얽힘 증류 가능성에는 영향을 주지 않는다.

위와 같은 양방향 양자 얽힘 증류 과정을 k번 거친 후에 식 (7)의 양자 상태에서 계수들의 분포는 다음과 같이 얻을 수 있다 [7]:

$$q_{ab}^{(k)} = \frac{\sum_{c_0,\cdots,c_{2^k-2}} q_{ac_0} \cdots q_{a,b-c_0-\cdots-c_{2^k-2}}}{\sum_j (\sum_k q_{jk})^{2^k}}$$

위 식에서 분자에 해당하는 식을 다음과 같이 더 전개하여 간략히 표현하고자 한다.

$$\sum_{c_0,\cdots,c_{2^k-2}} q_{ac_0}\cdots q_{a,b-c_0-\cdots-c_{2^k-2}}$$

$$=\sum_{c_0,\cdots,c_{2^k-1}} \delta_{c_{2^k-1},b-c_0-\cdots-c_{2^k-2}} q_{ac_0}\cdots q_{a,c_{2^k-1}}$$

크로네커-델타 함수의 다음의 표현을 이용하여

$$\delta_{c_{2^k-1},b-c_0-\cdots-c_{2^k-2}} = \frac{1}{d}\sum_l e^{-\frac{2\pi i}{d}l(b-c_0-\cdots-c_{2^k-1})}$$

양자 얽힘 증류 프로토콜 k번 반복 후 계수는 다음처럼 간략히 표현할 수 있다:

$$q_{ab}^{(k)} = \frac{\sum_l e^{-\frac{2\pi i}{d}lb}(\sum_c e^{\frac{2\pi i}{d}lc} q_{ac})^{2^k}}{d\sum_j(\sum_k q_{jk})^{2^k}} \quad (8)$$

위의 표현을 좀 더 자세히 표현할 수 있는데, 이를 위하여 다음의 몇 가지 변수를 정하자. 먼저 F 는 갑(A)과 을(B)이 각자의 비트를 측정할 때 모두 같은 값을 얻을 확률을 의미한다:

$$F = \sum_n p(A=B=n)$$

그리고 갑과 을의 측정값이 다를 때, 그 값들의 차이가 j만큼 다를 확률을 각각 다음처럼 나타내자:

$$D_j = \sum_n p(A=n, B=n+j)$$

따라서 다음이 성립함을 또한 기억하자.

$$F + \sum_{j\neq 0} D_j = 1$$

이제 다음의 두 변수들을 더 소개하여

$$C(m) = \frac{D_m}{F} \qquad A(m,l) = \frac{1}{F}\sum_j e^{\frac{2\pi i}{d}lj} q_{mj} \quad (9)$$

식의 계수들의 분포를 다음과 같이 표현할 수 있다.

$$q_{ab}^{(k)} = \frac{(C(a))^{2^k} + \sum_{l\neq 0} e^{-\frac{2\pi i}{d}lb}(A(a,l))^{2^k}}{d(1+\sum_{j\neq 0}(C(j))^{2^k})}$$

여기서 a=0, b=0 인 경우가 최대 얽힘 상태에 대응하는 계수이며 다른 계수들보다 크다는 사실을 기억하자. 만일 그렇지 않은 경우가 주어진다면, 갑과 을은 바일 연산자를 활용한 통신 수반-국소 연산 (LOCC)를 활용하여 a=0, b=0 에 해당하는 계수가 최대가 되도록 언제나 변환할 수 있다. 또한 다음이 성립하도록 변환 가능하다:

$$q_{0l}^{(k)} > q_{ml}^{(k)} \quad m \neq 0$$

이 조건은 다음을 의미한다.

$$A(0,l) > A(m,l) \quad m \neq 0 \quad (10)$$

이 조건들은 후에 보안성 조건을 구할 때 다시 사용될 것이다.

이제 양자 오류 정정 부호의 대상이 되는 비트-에러들과 위상-에러들을 다음과 같다.

$$R_D^{(k)} = \sum_{m\neq 0}\sum_n q_{mn}^{(k)}$$

$$R_P^{(k)} = \sum_m \sum_{n\neq 0} q_{mn}^{(k)}$$

최대 얽힘 상태가 얻어졌다면 위의 다음의 표현에 해당되는 위상-에러들은 다음과 같으며

$$Q_n^{(k)} = \sum_m q_{mn}^{(k)}$$

앞서 소개한 표현들을 사용하여 다음과 같이 나타낼 수 있다.

$$Q_n^{(k)} = \frac{1}{d} + \frac{E_n^{(k)}}{d(1+X^{(k)})}$$

여기서

$$E_n^{(k)} = \sum_m\sum_{l\neq 0} e^{-\frac{2\pi i}{d}ln}|A(m,l)|^{2^k}$$

$$X^{(k)} = \sum_{m\neq 0}|C(m)|^{2^k}$$

으로 사용였다. 비트-에러 수정을 충분히 수행하여 기대하는 비트-에러의 비율이 충분히 작은 임의의 숫자에 대해서 작도록 하고, 측정시 기저를 변환하여 위상-에러 또한 충분히 수행하여 임의의 작은 숫자에 대해서 작도록 한다. 임의로 작은 숫자 r 을 선택하여, 위상-에러의 비율이 임의의 작은 숫자 (epsilon)에 대해서 다음이 성립하도록 한다:

$$r \approx \frac{\epsilon}{R_P} = \epsilon(1+\frac{1}{X^{(k)}})$$

체르노프-호에프딩 (Chernoff-Hoeffding) 상한 공식에 의하여 위상-에러는 위의 변수들을 사용하여 다음의 상한을 갖게 된다.

$$R_P \leq \sum_{n\neq 0}(1-(\sqrt{Q_0^{(k)}}-\sqrt{Q_n^{(k)}})^2)^r$$

다음의 부등식을 적용하면,

$$(1-x)^r \leq e^{-rx}$$

위상-에러의 상한은 다음과 같이 전개된다:

$$R_P \leq e^{-r(\sqrt{Q_0^{(k)}}-\sqrt{Q_n^{(k)}})^2} = e^{-r(E_0^{(k)}-E_n^{(k)})^2/4d}$$

충분히 큰 k에 대하여 r은

$$r \approx \epsilon / X^{(k)}$$

을 만족하므로 k 번 프로토콜의 진행 후에 최종적으로 에러들은 다음과 같은 상한을 갖게 된다.

$$D_{mn}^{(k)} = R_D + R_P \leq \epsilon + \sum_{n \neq 0} \exp\left[-\frac{\epsilon (E_0^{(k)} - E_n^{(k)})^2}{4dX^{(k)}}\right]$$

위의 에러들은 k가 커짐에 따라 수렴하거나 발산하게 되는데 그 경계는 지수함수의 증가와 발산과 동일하다. 따라서 위의 지수함수는 다음의 조건을 만족할 때 매우 작은 수 (epsilon) 로 수렴한다:

$$\max_{n \neq 0} |E_0^{(k)} - E_n^{(k)}|^2 \geq X^{(k)} \tag{11}$$

위의 조건은 양방향 양자 암호 프로토콜의 보안성 조건, 즉 충분 조건이다. 다시 말하면, 위의 조건을 만족할 때, 양방향 양자 암호 프로토콜을 통해 비밀키를 얻을 수 있다.

위의 보안성 조건식 식 (110)을 양자 암호 프로토콜 적용시 직접 사용 가능한 조건으로 좀 더 변환해 보자. 먼저 좌변에 대해 다음의 전개를 활용하면

$$|E_0^{(k)} - E_n^{(k)}|^2 = |E_0^{(k)}|^2 \left(1 + \frac{E_n^{(k)} - 2\mathrm{Re}(E_0^{(k)*} E_0^{(k)})}{|E_0^{(k)}|^2}\right)$$

k가 커짐에 따라 두 번째 분수로 표현된 항은 점점 작아지고 다음과 같이 전개됨을 알 수 있다:

$$\begin{aligned} |E_0^{(k)} - E_n^{(k)}|^2 &\geq |E_0^{(k)}|^2 \\ &= |\sum_m \sum_{l \neq 0} e^{-\frac{2\pi i}{d} nl} (A(m,l))^{2^k}|^2 \\ &= |A_{ML}^{2^k} e^{-\frac{2\pi i}{d} nL}|^2 \times \\ &|1 + \sum_{m \neq M} \sum_{l \notin \{0,L\}} O[(\frac{A(m,l)}{A_{ML}} e^{-\frac{2\pi i}{d} n(l+L)})^{2^k}]|^2 \end{aligned}$$

여기서 다음의 변수를 사용하였다:

$$A_{ML} = \max_{m, l \neq 0} A(m,l)$$

식 (10)로부터 m=0인 경우 최대가 된다. 따라서

$$|E_0^{(k)} - E_n^{(k)}|^2 \geq \max_{l \neq 0} A(0,l) \tag{11}$$

보안성 조건식 (10)의 우변은 다음과 같이 전개된다.

$$X^{(k)} = (\max_i C(i))^{2^k} (1 + O((\frac{C(j)}{\max_i C(i)})^{2^k})) \tag{12}$$

식(9)로부터 보안성 조건 식 (10)은 다음과 같이 정리할 수 있다.

$$\max_{l \neq 0} |\frac{\sum_j q_{0j} e^{\frac{2\pi i}{d} lj}}{F}|^2 > \max_i \frac{D_i}{F} \tag{13}$$

식 (13)에서 구한 보안성 조건은 논문 [3]에서 보인 보안성 조건과 일치한다. 위의 보안성 조건은 d차원 양자계에 일반적으로 적용 가능하며 또한 가장 높은 수준의 채널 공격에 대한 보안성을 의미한다.

3. 특정 프로토콜에의 활용

식 (13)에서 보여진 보안성 조건은 일반적인 채널 공격에 대한 보안성을 의미하고 일반적인 준비-및-측정 프로토콜에 적용가능하다. 따라서 알려진 큐빗 활용 프로토콜들 BB84 프로토콜, six-state 프로토콜, 등에 적용할 수 있고, 이들을 일반화한 d 차원 프로토콜인 2-기저 프로토콜 및 (d+1)-기저 프로토콜에 적용할 수 있다.

보안성 조건	BB84 프로토콜	six-state 프로토콜
충분 조건	20%	27.6%
필요조건	25%	33.3%

조건이며 양자 얽힘은 양자 암호 프로토콜 성립의 필요조건이다. 즉, 양자 얽힘 없이 분리가능한 양자 상태로는 비밀키를 얻지 못함을 증명할 수 있다 [8]. 일반적으로 앞서 언급한 개별 공격들 (individual attacks) 에 대한 보안성 조건은 양자 얽힘과 일치해 왔다. 현재까지도 충분조건과 필요조건의 간격을 줄일 수 있는 지는 미해결 문제로 남아 있다. 예를 들어 BB84 프로토콜에 적용하였을 경우 보안성 조건은 20%이고, 양자 얽힘 조건은 25%이다. 25%이하의 양자 상태들은 고전 상관 관계에서 존재하지 않는 양자 상관 관계를 포함하고 있으나, 이 상관관계가 양자 암호의 보안성과 연결될 수 있을 지는 여전히 대답을 기다리고 있다.

양자 암호는 그 응용성 이외에도, 정보처리의 가장 기본 단위인 양자 시스템을 정보이론 및 정보 처리에 적용한다는 점에서, 정보-이론적으로도 매우 흥미롭다. 앞서 언급한 양자 암호의 충분 조건과 필요 조건의 간격이 좁아질 수 있는 지의 여부 또한 정보 이론에서 정보의 질적 분류에서 매우 중요하다. 양자 암호는 응용성 뿐 아니라 비밀 정보가 근본적으로 어떻게 정의되어야 하고, 그에 대응하는 물리적 원리들이 무엇인지, 그러한 보안성의 정의와 물리적 의미를 표현하는 수학적 전개, 논리 및 개념 소개와 정보-이론적 도구들의 개발하는 모든 과정을 수반한다. 양자 암호 이론은 높은 보안성을 지닌 통신 방법 개발을 통하여 새로운 정보 이론 및 새로운 정보 기술 패러다임을 만들고 있다.

Ⅲ. 결 론

본고에서는 양방향 양자 암호 프로토콜의 보안성을 재고하였다. 양방향 양자 암호 프로토콜의 첫 보안성 분석은 고테스만 (Gottesman) 과 로 (Lo) 의 양자 오류 정정 부호의 활용과 양자 얽힘 증류의 과정을 통해 얻어졌다. 이 보안성 조건은 2007년 논문 [3]의 정보론적 증명을 통해 개선되었다. 현재까지도 2007년의 결과는 양방향 양자 암호 프로토콜에서 가장 개선된 보안성 분석으로 알려져 있다. 본 논문에서는 2007년 논문 [3]에서 얻어진 개선된 양자 암호 프로토콜의 보안성을 고테스만 (Gottesman) 과 로 (Lo)가 논문 [2] 에서 사용했던 양자 오류 정정 부호 및 양자 얽힘 증류 조건들을 활용하여 재고하고, 2007년 논문 [3] 에서 얻어진 보안성 조건을 식 (13)에서 유도하였다.

고테스만 (Gottesman) 과 로 (Lo)의 접근 방식은 보안성 조건의 충분조건을 구하는 것이다. 반면 2007년 논문 [3] 에서는 충분 조건과 그에 해당하는 프로토콜에 대한 공격을 고려한 필요조건을 모두 제시하였다. 본 논문에서 얻은 보안성 조건 식 (13) 은, 고테스만 (Gottesman) 과 로 (Lo)의 접근 방식을 활용하였으므로, 논문 [3]의 충분 조건을 구한 것이다.

양자 암호의 보안성 증명은 일반적으로 최대 양자 얽힘을 증류하는 것과 동치이다. 이를 위해, 양자 오류 정정 부호, 양자 얽힘 증류, 정보-이론적 접근 방식, 양자 게임 이론, 등을 활용하여 최대 양자 얽힘 증류로의 환원을 보이는 것이 현대 암호의 관점에서 일반적인 방법이다. 본 논문에서는 양자 정보 이론의 전통적인 방법들 – 양자 오류 정정 부호, 양자 얽힘 증류, 정보-이론적 접근 – 을 재고하여 양방향 양자 암호 프로토콜의 보안성 조건을 재고하고 개선하였다.

참 고 문 헌

[1] Shor, P., Preskill, J. “Simple Proof of Security of the BB84 Quantum Key Distribution Protocol” Phys. Rev. Lett. 85, 441-444 (2000).

[2] Gottesman, D., Lo, H.-K., “Proof of security of quantum key distribution with two-way classical communications” IEEE Transactions on Information Theory, 49 (2) p. 457 (2003).

[3] Bae, J. Acin, A, “Key distillation from quantum channels using two-way communication protocols” Phys. Rev. A 75, 012334 (2007).

[4] Maurer U, “Secret Key Agreement by Public Discussion from Common Information ” IEEE Trans. Inf. Theory 39, 733 (1993).

[5] Bennett C. H., Brassard G., Popescu S., Schumacher B, Smolin J. A., Wootters W. K., “Purification of Noisy Entanglement and Faithful Teleportation via Noisy Channels”, Phys. Rev. Lett. 76 p722-725, (1996).

[6] Collins D, Popescu S, “A classical analogue of entanglement”, Phys. Rev. A. 65. 032321 (2002).

[7] Martin-Delgado M.A., Navascues, M “Distillation Protocols for Mixed States of Multilevel Qubits and the Quantum Renormalization Group” Eur.Phys.J. D 27 169-180 (2003).

[8] Acin. A, Gisin, N, “Quantum correlations and secret bits”, Phys. Rev. Lett. 94, 020501 (2005).

약 력

배 준 우

2001년 한양대학교 이학사
2003년 한양대학교 이학석사
2007년 바르셀로나 대학교 (Universitat de Barcelona) 이학박사
2007년~2011년 한국 고등과학원 (KIAS) 연구원
2011년~2014년 싱가포르 국립대학 양자 정보 센터 (Centre for Quantum Technologies) 및 바르셀로나 ICFO (Institut de Ciencies Fotonique) 양자 정보 이론 그룹 연구원 (공동)
2014년~2015년 독일 프라이부르크 고등과학원 (Freiburg Institute for Advanced Studies, FRIAS), 주니어 펠로우 (연구책임자)
2015년~현재 한양대학교 응용수학과 교수