情 報 保 護 學 會 誌
第 14 券 第 3 號, 2004. 6

양자 암호(Quantum cryptography)

김 재 완*

요 약

양자물리학은 디지털통신보안에 대해 '병 주고 약 주는' 관계에 있다. 양자컴퓨터는 디지털컴퓨터로는 풀기 어려운 문제를 쉽게 풀 수 있을 것으로 기대되어, 어려운 수학 문제에 그 보안성을 담보하는 공개키 암호체제가 양자컴퓨터의 위협 앞에 놓이게 된 한편, 양자물리학은 일회용난수표를 도청이 절대 불가능한 방식으로 전송하는 양자암호기술이라는 새로운 형태의 암호체제를 제시한다. 양자암호기술은 기존의 암호기술과 함께 21세기 디지털통신에 완벽한 보안대책을 제공하게 될 것이다.

Ⅰ. 서 론

양자물리학과 디지털보안은 '병(病) 주고 약(藥) 주는' 관계에 있다.

1. 양자 물리학과 관련된 디지털 보안의 위협

1970년대에 개발된 공개키 암호체제는, 풀기 어려운 문제를 공개키(자물쇠)로 사용하여 암호문을 만들고, 그 문제의 해답을 비밀키(열쇠)로 사용하여 암호를 풀 수 있도록 되어 있다. 공개키로 많이 사용되는 풀기 어려운 문제는 큰 수의 소인수분해이다. 이 방식을 고안한 Rivest, Shamir, Adleman(RSA) 등 세 사람은 1977년 Scientific American에 129자리 자연수를 소인수분해하라는 100달러짜리 현상금 문제를 냈다. Rivest는 하드웨어의 발달까지 고려하여 4경(4×10^{16}) 년이 걸릴 것이라고 예상했으나, 1994년 25 개국 600여 자원봉사자의 1600 대에 달하는 각종 컴퓨터를 8 개월간 동원한 노력 앞에 풀리고 말았다. 이는 정수론의 발달로 발견된 새로운 알고리듬 덕분에 가능했던 것이다. 그러나 여전히 소인수분해 문제는 문제의 크기에 거의 지수함수에 가까운 정도의 시간이 소요되는 어려운 문제이다. 한 계산에 의하면, 2000자리 자연수의 소인수분해는, 우주 전체의 입자들 수효(10^{80}개)만큼의 컴퓨터를 우주의 나이(10^{18}초) 동안 사용해도, 할 수 없다고 한다. 공개키 암호체제의 이렇게 굳건해 보이던 안전성은 양자컴퓨터의 출현가능성 앞에 허물어지게 되었다. 1994년 AT&T의 Shor는 양자컴퓨터를 사용하면 소인수분해 문제는 문제크기의 지수함수가 아니라 세제곱정도의 시간에 풀릴 수 있다는 걸 증명했다. 따라서 현재 이용되고 있는 RSA 방식 공개키 암호체제는 양자컴퓨터가 본격적으로 개발되는 그 날로 완전무장해제가 되는 셈이다. (양자컴퓨터가 아니라 하더라도, 아직 우리가 알지 못하는 새로운 알고리듬으로 공개키 암호체제가 무너질 가능성도 무시할 수 없다.)

2. 양자 물리학과 관련된 디지털 보안

양자컴퓨터가 공개키 암호체제에 치명적인 위협으로 등장하고 있지만, 양자물리학을 이용한 양자암호기술은 이를 극복할 절대적인 통신보안의 새로운 수단으로 증명되었다. 일회용난수표를 열쇠와 자물쇠로 사용하는 대칭암호체제는 절대보안성이 증명되어 있긴 하지만, 그건 두 통신당사자가 일회용난수표를 안전하게 나누어가지고 있을 경우에만 해당하는 이야기다. 난수표를 두 번 이상 사용하면 메시지는 물론 난수표까지 노출될 가능성이 있으므로, 통신당사자들은 계속하여 새로운 난수를 나누어가져야 한다. 요즘은 뜸해졌지만, 간첩수사발표에서 난수표가 단골메뉴로 등장하는

* 고등과학원 계산과학부 교수 (jaewan@kias.re.kr)

것처럼, 난수표를 통신당사자들이 절대적으로 안전하게 나눠가진다는 것은 기존의 방법으로는 불가능하다. 양자암호기술은 난수표를 두 통신당사자가 양자물리학을 이용하여 절대적으로 안전하게 나눠가질 수 있는 방법이다.

RSA연구소의 연구팀장인 Kaliski는 "양자암호기술은 암호기술의 주요한 패러다임 변혁"이라고 하면서, "기존암호기술과 양자암호기술의 결합은 더욱 안전한 통신체계를 실현하는 강력한 도구"라고 한다.

II. 양자 역학의 특성

1. 큐비트의 양자 정보체계

수학의 실수(real number)체계가 복소수(complex number)체계로 확장되는 것처럼, 비트(bit)로 표현되는 디지털정보체계는 양자비트(quantum bit) 또는 큐비트(qubit)의 양자정보체계로 확장된다. 디지털정보와 양자정보의 다른 점을 비교해보자.

비트는 0 또는 1 두 상태 중 하나이지만, 큐비트는 $|0>$과 $|1>$이 중첩된 상태에 있게 된다. N 개의 비트는 00...0부터 11...1까지 2^N가지의 가능성 중 하나만 나타낼 수 있지만, N 개의 큐비트는 $|00...0>$부터 $|11...1>$까지 2^N가지 모두가 중첩된 상태를 나타낼 수 있다. 이렇게 큐비트 개수에 대해 지수함수적으로 늘어나는 기억 및 계산공간 덕분에 양자컴퓨터는 디지털컴퓨터보다 더 크고 더 빠른 계산을 할 수 있다.

2. 복사불가능한 양자 정보, 비가역적인 양자측정

디지털정보는 얼마든지 복사가 가능하지만, 양자정보는 복사가 불가능하다.

예를 들어, $|\alpha>$와 $|\beta>$를 각각 복사하여 각각 $|\alpha>|\alpha>$와 $|\beta>|\beta>$가 된다고 가정하면, $|\alpha>+|\beta>$를 복사하려고 할 때에 $(|\alpha>+|\beta>)(|\alpha>+|\beta>)$처럼 복사가 되지 않고, 양자물리학의 선형성 때문에 $|\alpha>|\alpha>+|\beta>|\beta>$로 되어 양자 얽힘 상태가 된다. 얽힘 상태는 두 개별 상태의 곱으로 표시될 수 없는 상태를 가리킨다.

만약에 양자정보를 복사할 수 있게 되면 20세기 물리학의 두 기둥, 양자물리학과 상대성이론이 무너지게 된다. 우선 모르는 양자상태를 무수히 복사하여 원하는 대로 측정하면 그 양자상태에 대해서 정확히 알 수 있게 되는데, 이는 양자물리학의 불확정성 원리에 어긋난다. 또한 양자얽힘의 비국소적인 성질을 이용하고 양자정보를 복사할 수 있으면, 빛보다 빠른 통신이 가능해지는데, 이는 상대성이론에 정면으로 모순이 된다.

디지털정보는 읽힐 때에 그 상태가 변하지 않지만, 양자정보는 읽힐 때에 즉 측정될 때에 돌이킬 수 없게 그 상태가 달라질 수 있다. 예를 들어, $|\pm>=\frac{|0>\pm|1>}{\sqrt{2}}$ 상태를 $|+>$나 $|->$상태 둘 중 어느 상태인지 알아내기 위해 읽는다면(측정한다면) $|+>$ 또는 $|->$ 상태 그대로 머물러 있지만, $|0>$ 또는 $|1>$ 둘 중에 어느 상태인지 알아내기 위해 읽는다면 원래대로 $|+>$나 $|->$상태가 아니라, 각각 50%의 확률로 $|0>$ 또는 $|1>$의 상태로 측정되고 측정된 직후에도 그 변한 상태대로 있게 된다.

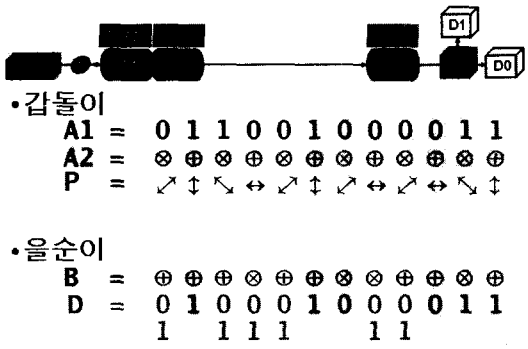
III. 양자 암호 기술

양자정보의 복사불가능성과 양자측정의 비가역성을 이용하면 양자암호기술을 이해할 수 있다. 갑돌이가 을순이에게 양자정보를 보낼 때에 중간에서 도청하는 방법은 두 가지로 생각해 볼 수 있다. 하나는 통신채널로 지나가는 양자정보를 복사하는 것인데, 이는 앞에서 밝힌 대로 불가능하다. 다른 방법은 지나가는 양자정보를 살짝 끄집어내어 읽어(측정해) 보고 도로 통신채널에 집어넣어 을순이에게 가도록 하는 것인데, 이렇게 하면 갑돌이가 보낸 양자정보와 을순이가 받는 양자정보가 달라질 수 있다. 갑돌이와 을순이는 주고받은 양자상태 중 일부를 공개적으로 비교해 봄으로써 도청 가능성을 알아낼 수 있다.

IBM의 Bennett과 몬트리올대학교의 Brassard가 1984년에 고안한 BB84로 불리는 양자암호기술(양자암호키전송)은 다음과 같다.

갑돌이가 을순이에게 단일광자(single photon)를 보내는데, ↔, ↕(+방식 : 수평 또는 수직 편광방식), ↗, ↖(×방식 : 45도 또는 135도 대각선 편광방식) 등 네 가지 편광상태 중에서 하나로 만들어 보낸다. 이렇게 하기 위해 갑돌이는 각각 50% 확률로 0 또는 1이 나오게 하는 난수발생기(random number generator) 두 개를 사용한다. 첫 번째 난수발생기는 을순이에게 보낼 비트 0 또는 1을 결정하고, 두 번째 난수발생기는 이 비트를 코딩할 편광방식 +방식 또는 ×방식을 결정한다. 예를 들어, 갑돌이의 두 난수

가 0과 0이라면 비트 0을 +방식으로 코딩하여 ↔편광의 단일광자를 을순이에게 보내게 된다. 01은 0을 ×방식으로 코딩하여 ↗편광을, 10은 1을 +방식으로 코딩하여 ↕편광을, 11은 1을 ×방식으로 코딩하여 ↖편광을 보낸다.



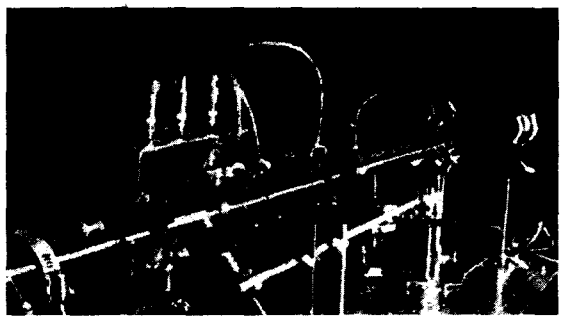
〔그림 1〕 BB84 양자암호전송. 갑돌이는 수평편광 단일광자를 발생시킨 후, 첫 번째 난수가 0이면 0도, 1이면 90도 포켈셀을 이용하여 편광을 회전시키고, 두 번째 난수가 0이면 0도, 1이면 45도 편광을 회전시킨 후 을순이에게 보낸다. 을순이는 난수가 0이면 0도, 1이면 -45도 편광을 회전시킨 후, 편광 빛살가르개(polarizing beam splitter)를 사용하여 측정한다. 편광 빛살가르개는 수평편광은 그대로 통과시키고 수직편광은 반사시켜 90도로 진행경로를 꺾어 보낸다. 갑돌이가 보낸 편광방식과 을순이가 읽는 편광방식이 같으면, 두 사람의 비트는 항상 같게 된다.

을순이도 난수발생기를 사용하여, 0이 나오면 +방식, 1이 나오면 ×방식으로 갑돌이가 보내온 단일광자의 편광을 측정한다. 을순이의 편광 측정 결과가 ↔ 또는 ↗이면 을순이는 갑돌이가 보낸 비트를 0으로 해석하고, ↕ 또는 ↖이면 1로 해석한다.

갑돌이가 보낸 편광방식과 을순이가 측정하는 편광방식이 같으면, 갑돌이가 보낸 비트와 을순이가 해석한 비트는 똑같은 것이 되고, 두 사람의 편광방식이 다르면 두 사람의 비트는 50%의 확률로 같을 수도 있고 다를 수도 있다. 예를 들어, 갑돌이의 난수쌍이 01이면 갑돌이는 ↗편광을 보낸다. 이 때에 을순이의 난수가 1이라서 갑돌이와 똑같은 편광방식인 ×방식으로 측정하면 100%의 확률로 ↗편광을 얻게 되고, 을순이는 이를 갑돌이가 보낸 비트와 같은 0으로 해석하게 된다. 그렇지만 을순이의 난수가 0이라면 을순이는 +방식으로 측정하게 되는데, ↗편광은 +방식으로 측정할 때에 50%의 확률로 ↔로 측정되기도 하고 ↕로 측정되기도 한다. 을순이는 이를 0 또는 1로 해석하게 되어, 갑돌이가 보낸 비트를 맞출 확률이 50% 밖에 되지 않는다.

두 사람 사이의 단일광자 전송이 끝나면, 두 사람은 보낸 상태나 읽은 상태, 즉 비트는 공개하지 않고, 보낸 방식과 읽은 방식만을 공개적으로 비교한다. 갑돌이가 보낸 방식과 을순이가 읽은 방식이 같으면 두 사람은 똑같은 양자상태를 인식하게 되므로 이를 이용하여 대칭비밀키를 만들면 된다.

앞에서 말한 대로 양자통신채널을 도청하기 위해 통신채널로 지나가는 양자상태를 복사하는 것은 불가능하다. 또 다른 도청방식으로 도청자가 중간에서 양자상태를 읽는다면, 갑이 보낸 편광방식과 을이 읽는 편광방식은 같고 도청자의 편광방식만 다르다면, 50%의 확률로 같아야 할 갑돌이와 을순이의 비트가 달라지게 된다. 따라서 갑돌이와 을순이는 두 사람의 편광방식이 같은 것들 중에서 몇몇을 골라 정말로 두 사람의 비트가 같은지 확인해 봄으로써 도청여부를 가늠해 볼 수 있다. 서로 다른 경우가 너무 많으면 통신채널의 이상이나 도청가능성을 의심해보아야 한다. 보낸 방식과 읽는 방식이 다를 경우에는 두 사람이 인식하는 양자상태 사이에 아무런 상관관계가 생기지 않으므로 무시한다.



〔그림 2〕 세계최초의 양자암호키전송. 1989년 IBM의 Bennett 등. 32cm 거리에 있는 두 송수신 장치 사이에 4가지 편광 상태를 이용한 양자암호키전송을 성공시켰다.

Bennett 등은 1989년 32 cm 거리에서 최초의 양자암호통신실험에 성공했다. 최근 도시바는 광섬유로 100 km 거리에 양자암호키를 전송하는 데에 성공했다. 유럽의 Rarity 등과 미국 로스알라모스연구소의 Hughes 등은 각각 23 km와 10 km 대기 중에서 양자암호키전송에 성공하였는데, 이는 장차 위성통신에 양자암호기술을 적용할 전단계 실험에 해당한다.

한편 미국의 벤처회사인 MagiQ와 스위스의 벤처회사인 IDQuantique은 상업용 양자암호시스템을 2003년 현재 시판 중이라고 광고하고 있다. 특히 IDQuantique의 Gisin교수는 Swiss Telecom과 Geneva 대학교에서 현재 제네바와 로잔 사이에 설치되어 있는 광통신용 광섬유를 이용하여 67km의 거리에서 양자암호통신을 하는 데에 성공한 바 있다.

Ⅳ. 양자원격전송(quantum teleportation)

BB84 방식의 양자암호기술은 단일광자를 전송해야 하는데, 단일광자는 광섬유를 통해서 전송되는 중에 양자상태가 깨어지거나 광자가 아예 광섬유에 흡수되어 사라질 수도 있다. 기존의 광통신에서는, 광신호가 약해지거나 잡음을 타기 전에, 일정한 거리를 지나 온 광신호를 증폭함으로써 광신호의 질을 유지한다. 증폭이란 일종의 복사(copy)와 같은 과정으로서, 복사가 불가능한 양자상태에는 적용할 수 없다. 양자통신에서는 이러한 증폭 대신, 앞에 잠깐 설명한 양자얽힘을 이용하여, 주어진 양자상태를 복사하거나 읽어보지 않고 멀리 전송하는 양자원격전송(quantum teleportation)이 가능하다.

멀리 떨어져 있는 병호와 정숙이가 양자얽힘(quantum entanglement), 즉 양자물리학적으로 상관관계를 가진 한 쌍의 양자상태를 가지고 있다고 하자. 이때 병호와 정숙이가 각각 가지고 있는 양자상태는 측정되기 전까지 어떤 상태인지 정해져 있지 않지만, 어느 한 쪽이라도 측정이 이루어지면 양쪽의 측정결과가 '고전물리학으로는 설명할 수 없는' 상관관계를 순간적으로 가지게 된다. 아인슈타인은 이렇게 멀리 떨어져 있는 두 양자상태 측정 사이의 순간적인 상관관계가, 빛보다 빠른 것은 있을 수 없다는 특수상대성이론의 가정과 배치되는 '유령 같은 원격작용'이라고 거부했다. 그러나, 이제 양자얽힘이 가진 이러한 양자상관관계는 실험적으로 잘 증명되어 있다. 그렇지만 양자측정의 결과는 확률적으로 정해지기 때문에, 양자얽힘의 상관관계를 써서 자의적인 신호를 빛보다 빠른 속도로 보낼 수 있는 것은 아니어서, 아인슈타인이 염려했던 것처럼 특수상대성이론과 모순이 되는 것도 아니다.

이제 이 양자얽힘의 양자상관관계를 이용하여 병호는 정숙이에게, 자신이 가지고 있지만 모르는 양자상태를 보낼 수 있는데, 이를 양자원격전송(quantum teleportation)이라고 한다. 이때에 병호는 정숙이에게 그 양자상태를 완전히 나타내기에는 턱없이 부족한 정보를 일반통신채널을 통해 보낼 필요가 있다. 이런 상황은 마치 아주 가까운 두 사람이 경험하는 이심전심(以心傳心)과 비슷하다. 두 사람이 공유한 경험이 많이 있으면, 한 사람이 다른 사람에게 한 마디만 툭 던져도, 상대방은 그 깊은 뜻을 알아차릴 수 있는 법이다. 여기서 양자얽힘은 두 사람이 공유한 경험에 비유할 수 있다.

멀리 떨어져 있는 통신당사자들은 중간에 디지털정보에서처럼 증폭장치를 사용할 수는 없지만, 양자중계기(quantum repeater)를 두고 통신당사자와 양자중계기들 사이에 양자얽힘을 이용한 양자원격전송을 함으로써 원거리 양자통신이 가능하고, 원거리 양자암호키전송도 할 수 있다.

Ⅴ. 결 론

양자암호기술은 양자정보처리 분야에서 가장 일찍 실현될 수 있는 기술로서, 양자컴퓨터를 비롯한 더 광범위한 양자정보과학기술의 기초가 된다. 양자암호기술을 실현하기 위해서는 단일광자나 기타 양자광 상태의 발생, 조작, 전송, 측정 등을 비롯한 양자광학적인 기술의 발달과 양자오차수정을 비롯한 양자정보과학의 발전이 절실히 요구된다. 지난 십수년간 IT 강국으로 발돋움한 우리나라가 앞으로 다가올 양자정보분야에서도 기술적 우위를 지키기 위해서는 이 분야 연구에 대해 많은 관심이 필요하다.

참 고 문 헌

[1] 최근 양자정보처리 전반에 관한 전문서과 일반 교양서적들이 많이 출판되었으며, 리뷰논문들도 많이 찾아 볼 수 있다.

[1-1] M. A. Nielsen and I. L. Chuang, Quantum Computation and Quantum Information, Cambridge Press, Cambridge (2000)

[1-2] D. A. Ekert, and A. Zeilinger, Eds., The Physics of Quantum Information, Spring-Verlag, Berlin (2000)

[1-3] C. P. Williams and S. H. Clearwater, Explorations in Quantum Computing, Springer-Verlag, New York (1998)

[1-4] J. Brown, Minds, Machines, and the

Universe, Simon & Schuster, New York (2000)
[1-5] H.-K. Lo, S. Popescu, and T. Spiller, Introduction to Quantum Computation and Information, World Scientific, Singapore (1998)
[1-6] D. Gottesman and H.-K. Lo, Physics Today, Nov. 2000, 22
[1-7] S. J. Lomonaco, Jr., quant-ph/0102016
[1-8] N. Gisin et al., quant-ph/0101098
[2] 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, 1484 (1997). And also quant-ph/950827.
[3] C. H. Bennett, G. Brassard, C. Crepéau, R. Jozsa, A. Peres, and W. K. Wooters, Phys. Rev. Lett. 70, 1895 (1993).
[4] C. H. Bennett and S. J. Wiesner, Phys. Rev. Lett. 69, 2881 (1992).
[5] W. K. Wooters and W. H. Zurek, Nature (London) 299, 802 (1982).
[6] C. H. Bennett and G. Brassard, in Proc. IEEE Int. Conference on Computers, Systems and Signal Processing, IEEE, New York (1984), p.175. C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, J. Cryptol. 5, 3 (1992).
[7] C. H. Bennett, Phys. Rev. Lett. 68, 3121 (1992).
[8] A. K. Ekert, Phys. Rev. Lett. 67, 661 (1991).
[9] A. K. Ekert, J. G. Rarity, P. R. Tapster, and G. M. Palma, Phys. Rev. Lett. 69, 1293 (1992).
[10] B. Huttner, N. Imoto, N. Gisin, and T. Mor, Phys. Rev. A 51, 1863 (1995).
[11] R. Hughes, G. Morgan, and C. Peterson, Jour. Mod. Opt. 47, 533 (2000).
[12] W. T. Buttler, R. J. Hughes, S. K. Lamoreaux, G. L. Morgan, J. E. Nordholt, and C. G. Peterson, Phys. Rev. Lett. 84, 5652 (2000).
[13] S. J. D. Phoenix, S. M. Barnett, P. D. Townsend, and K. J. Blow, Jour. Mod. Opt. 42, 1155 (1995). E. Biham, B. Huttner, and T. Mor, Phys. Rev. A 54, 2651 (1996).
[14] P. W. Shor and J. Preskill, Phys. Rev. Lett. 85, 441 (2000).

〈著 者 紹 介〉

김 재 완 (Jae-Wan Kim)

1977~1985년 : 서울대학교 물리학 학사
1985~1993년 : University of Houston 물리학 박사
1993~1994년 : Texas Center for Superconductivity 포스닥연구원
1994~2002년 : 삼성종합기술원 전문연구원
2000~2002년 : 한국과학기술원 물리학과 부교수(연구교원)
2002~2004년 현재 : 고등과학원 계산과학부 교수