선진국 암호체계 뛰어넘을 열쇠 찾았다

글 _ 김칠민 배재대학교 물리학과 교수 chmkim@mail.pcu.ac.kr

광혼돈현상제어연구단은 혼돈의 응용에 연구의 초점을 맞춰 1998년 과학기술부의 창의적 연구진흥과제 중 하나로 연구를 시작했다. 광학계에서 생기는 다양한 혼돈 현상을 조사하고 이를 제어하며 응용하는 일들을 수행하고 있다. 그 일 중의 하나가 혼돈을 이용하여 새로운 암호 방법을 개발하는 것이다. 이 방법은 보내고자 하는 데이터를 혼돈 신호 속에 숨기면 혼돈 신호의 불규칙한 특성 때문에 외부의 공격자는 이 문서를 해독할 수 없게 된다. 따라서 이 방법은 암호의 체계상 비밀키 암호에 속하게 된다.

공개키 암호의 원리는 소인수분해

비밀키 암호란 일반적으로 말하는 암호로 문서를 남이 모르는 비밀 값(패스워드)으로 문서를 암호화하는 방법이다. 그런데 상대방에게 이 비밀문서를 전달할 때 비밀 값이 무엇인지를 알려주어야 하는데 이 비밀 값을 알려주는 것으로 고안된 암호법을 '공개키 암호'라 한다.

이 같은 분류에 따르면 암호는 체계상 커다란 세 가지 체계로 나뉘게 된다. 먼저 암호 데이터를 암호화하는 비밀키와 이 비밀키(패스워드)를 전송할 수 있는 암호시스템인 공개키와 그 비밀키 값으로 암호화한 데이터가 복원되면 어떤 값이 되는지를 나타내는 전체 데이터의 요약을 나타내는 해쉬 값이 있다. 이 해쉬 값을 만드는 암호를 해쉬함수라 한다. 공개키 암호는 전체 암호문 송수신의 제일 중요한 부분을 차지하고 있다.

이런 체계를 이용하여 갑이 을에게 문서를 암호화하여 보내는 방법을 생각하자. 갑이 을에게 어떤 문서를 보내고자 할 때 갑은 문서를 어떤 암호키 값으로 암호화한다. 을이 이 암호문을 풀려면 이 때 패스워드와 같은 암호키 값을 알아야 하는데 갑은 이 값을 그냥 알려줄 수가 없게 된다. 이유는 이 값을 중간에서 가로채는 사람은 누구나 그 값을 알 수 있어서 문서를 해독할 수 있기 때문이다. 이런 폐단을 없애기 위해 개발한 것이 공개키 암호다.

공개키는 두 개의 열쇠가 있어 한 열쇠로 문서를 암호화하여 잠그면 반드시 다른 열쇠로 열어야 한다. 공개키란 그 중 하나의 열쇠는 공개하고 다른 열쇠는 자기가 개인적으로 보관하며 남에게 공개하지 않는다. 이 때 공개키로 잠근 패스워드는 공개된 공개키로는 절대 열 수 없고 반드시 을이 개인적으로 보관하고 있는 개인키로 열어야 한다. 이 공개키 원리를 수학적으로 뒷받침하는 것이 소인수분해다. 공개된 키 값을 가지고 을이 개인적으로 보관하고 있는 개인키의 값을 알려면 엄청나게 긴 시간을 요하기 때문이다. 공개키 암호는 안전한 암호 방법이긴 하지만 데이터를 암호화하고 복호화하기에 시간이 너무 많이 걸리고 키 값이 너무 길다.

이렇게 긴 시간으로 인해 일반적인 데이터는 공개키로 암호화하지 못하고 비밀키를 암호화하는데만 주로 쓰이고 있다. 그래서 갑은 공개된 을의 열쇠를 이용하여 보내고자 하는 암호 문서의 패스워드를 암호화하여 을에게 보내면 을은 자기가 보관한 개인키를 이용하여 갑이 보낸 패스워드를 구한다. 그런 다음 갑은 보낼 문서를 을에게 보낸 비밀키(패스워드)로 잠가 을에게 보내고, 을은 자신의 개인키로 연 패스워드를 이용하여 문서를 복원하는 것이다.

이 때 그 문서의 변조 여부를 확인하기 위하여 갑은 암호 문서의 끝에 문서의 요약문을 보낸다. 을이 만약 문서를 변조나 제 삼자가 위조를 하면 해쉬 값의 결과가 완전히 달라져 암호문의 위변조를 확인하는 것이다.

RSA 암호 시스템 뛰어넘은 양자 컴퓨터

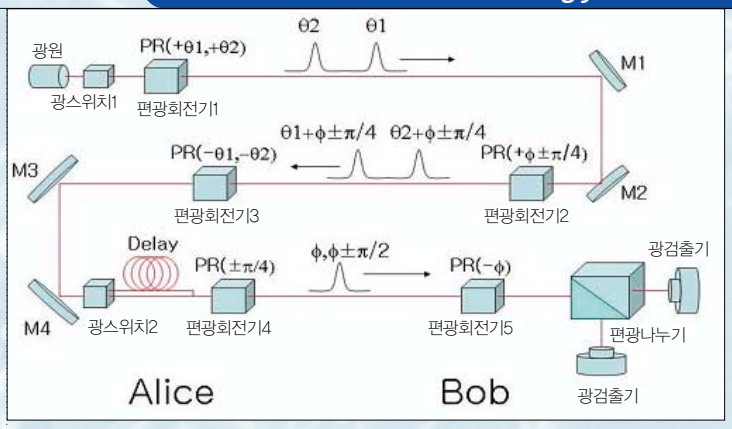
그런데 이런 암호 체계에서 가장 중요한 비밀키를 보내는 공개키 암호 방법에 최근 문제가 생기기 시작했다. 공개키 암호로 가장 일반적으로 쓰이는 RSA(Rivest Shamir Adleman)시스템은 소인수분해를 이용한 암호법인데 이 방법은 양자 컴퓨터가 발달하면 그 안정성을 보장받지 못하기 때문이다. 그 이유는 기존의 컴퓨터로 몇 년이 걸려도 분해하기 어려운 소인수에서 얻는 수를 미국 벨연구소의 수학자 피터 쇼어(Peter Shor)가 양자컴퓨터로 그의 알고리즘을 이용해 하루 안에 얻을 수 있다는 것을 지난 1994년 밝혀냈기 때문이다.

2년 후 같은 벨연구소 소속 로브 글로버 박사는 데이터 검색 알고리즘을 쓰면 양자 컴퓨터는 소인수분해를 할 것도 없이 '무식하게' 1부터 대입하여 구하여도 몇 분이면 해독의 열쇠를 알 수 있는 능력이 있다는 것을 밝혔다. 공개키를 이용하여 암호화한 패스워드는 공격자가 순식간에 그 패스워드를 알 수 있어 전송되는 데이터를 받아 암호문을 복원할 수 있는 것이다. 이 같은 획기적인 '사건' 이후 각 정부는 정부차원에서 양자 전산연구를 지원하기 시작했고 아울러 양자 전산의 암호 해독 능력을 피할 수 있는 양자암호를 개발하기 시작했다.

이 같은 과정에서 양자암호 개발에 관심을 갖기 시작했다. 혼돈을 이용한 암호체계를 연구하던 중, 혼돈 암호보다 더욱 본질적인 문제는 이런 양자 전산에 의한 공격으로 공개키 방법의 암호체계에 손질이 필요하다는 것을 알게 됐기 때문이다. 이런 공개키 암호에 기초한 고전 암호체계 방법의 개선을 어떻게 시작하느냐 하는 의문의 해답은 고전적 공개키를 대치할 수 있는 양자 암호의 개발일 수밖에 없었다. 따라서 연구단이 보유한 지식인 혼돈 암호체계와 광 혼돈, 양자 혼돈의 기술을 어떻게 접속시킬 것인가 하는 의문에서 연구는 시작됐다.

고전 암호 알고리즘 획기적 진전 가져와

먼저 연구단은 아직까지 실용화할 수 있을 만한 많은 광자 수를 이용한 안전한 양자 암호 방법이 아직 개발되지 못했음을 알게 됐다. 그래서 혼돈의 불규칙한 신호로 양자 암호에서 쓰이는 빛의 편광 방향을 어떻게 하면 상대방이 모르게 바꿀 수 있을까 연구하기 시작했다.



개발된 양자 암호 방법. 앨리스와 밥은 빛의 편광을 불규칙하게 회전시키고 풀어서 외부의 공격자들이 빛의 편광 상태를 모르게 한다. 또한 두 개의 빛 다발을 사용하여 그 중 하나를 불규칙하게 막음으로써 어느 빛 다발을 막았는지 모르게 하여 외부의 공격을 차단할 수 있다.

하지만 불규칙한 방향으로 편광의 방향을 바꿔주더라도 대화 상대방에서는 이를 쉽게 데이터를 복원할 수 있지만 제3자는 이를 찾을 수 있는 방법이 없음을 곧 깨닫게 됐고, 그 일이 가능한지를 조사했다. 그런 이후 이 암호의 안전성을 증명하기 위하여 각종 양자 암호에 대한 공격으로부터 안전성을 유지하기 위해 양자 암호를 보완하는 수순을 밟아 갔다. 전체 알고리즘이 완성되자 이제는 이것의 안정성을 양자광학적으로 증명하는 일이 남게 됐다. 그것은 불규칙하게 바꾼 편광을 어떻게 공격자가 찾을 수 있으며, 공격자가 이를 찾기 위해서 얼마만큼의 광자 수가 필요한지를 계산하는 일이었다. 이 양이 결정되면 이보다 작은 광자 수로 통신을 했을 경우 암호의 안전성도 유지되고, 다른 양자 암호 방법보다 많은 양의 광자를 쓸 수 있으므로 신호의 효율이 증가할 것이기 때문이었다. 이 같은 과정을 통해 암호의 안전성을 확보할 수 있었다. 개발된 암호를 발표하자 곧 이에 대한 공격이 세계적으로 시작됐고, 모든 공격 중 흉내내기 공격에 이 암호 방법이 가장 취약한 것으로 드러났다. 이에 대한 보완이 필요하여 서강대학교의 박영재 교수와 함께 그 취약점을 완전히 보강하여 흉내내기 공격뿐만 아니라 다양한 공격 방법에 대해서도 안전한 발전된 양자암호 방법을 발전시켰다.

이런 양자 암호는 앞으로의 암호에서 중요한 역할을 할 것으로 기대된다. 그 이유는 기존의 암호시스템은 현재 개발중인 양자 컴퓨터가 개발되면 더 이상 암호로서의 역

할을 하기 힘들기 때문이다. 벨연구소의 쇼어와 글로버가 개발한 양자 컴퓨터를 이용한 고전 암호에 대한 공격은 그 성능이 매우 우수하여 수학적 복잡성에 기반한 고전 암호 알고리즘이 더 이상 그 안전성을 확보하지 못하기 때문이다.

미국 정부 · 민간 나서서 암호체계 개발

현재 세계에서는 공개키를 기반으로 암호화하고 있는데 공개키는 모두 알려져 있어 양자 컴퓨터가 완성되는 순간 양자 컴퓨터를 가지고 있는 사람은 이 공개키를 이용하여 개인의 개인키를 금방 알 수 있고, 그러면 공개키를 믿고 암호화한 수많은 암호화 정보들과 보관되어 있는 수많은 과거의 비밀 정보들이 그대로 드러나게 된다. 예를 들어 양자 컴퓨터가 만약 10년내에 개발되고 양자 암호가 5년내에 개발된다면 양자 암호가 완성되기 전에 이루어진 모든 암호는 공격자가 모두 알게 된다. 그런데 양자 컴퓨터가 완성되는 그때도 양자 암호를 쓰지 않는 사람은 자신의 문서를 양자 컴퓨터를 가진 사람에 대하여 암호 없이 문서를 그대로 보내는 것과 같기 때문이다. 또한 글로버 알고리즘을 이용하면 이것을 수학적으로 풀 필요도 없이 그 값을 대입시키면 금방 공개키에서 개인키 값을 알 수 있기 때문에 공개키 자체가 무의미하게 된다. 그런데 공개키 없이는 현재 대부분의 암호는 존재할 수 없으므로 이는 심각한 문제가 되어 개인의 정보 유출은 말할 것도 없고 국가의 비밀 유지 자체도 난관에 봉착할 수 있다. 그래서 선진국에서는 이 문제를 빨리 해결하고자 양자 암호의 개발과 양자 컴퓨터의 개발에 박차를 가하고 있다. 이는 먼 미래의 일이 아니라 곧 닥치게 될 정보 보호의 심각한 문제가 될 수 있기 때문이다.

미국은 현재 이 같은 암호 체계의 개발에 중앙정보국(CIA), 국가정보국(NSA), 국방부 그리고 육 · 해 · 공군이 모두 연구비를 지원하고 있다. 또 로스알라모스연구소, 항공우주국, 표준연구소 등과 같은 국립 연구소뿐만 아니라 벨연구소, IBM 등 쟁쟁한 회사연구소들이 암호 체계 개발을 주도하고 있다. 양자전산의 실제 하드웨어 구현은 1995년 미국 표준연구소에서 이온 덫을 가지고 처음 시연한 이후 많은 물리적 시스템에서 양자 전산의 가능성이 발견되고 있고, 이런 연구들이 조직적으로 활발히 연구되고 있으므로 생각보다 빠르게 양자 전산이 실용화될 수 있다.

양자암호 개발의 키워드 '양자 얽힘'

이런 양자 전산의 가능성으로 인해 양자 암호의 개발에 많은 노력을 기울인 결과, 많은 양자 암호 방법들이 개발되었는데 이는 크게 두 가지로 나뉜다.

하나는 광자의 편광을 이용하는 방법이고 다른 하나는 '양자 얽힘' 상태를 이용하는 것이다. 빛을 이용함에 있어 빛의 개수가 우리가 셀 수 있는 양만큼 적어지면 이제는 이것이 양자문제로 귀결되고 이제는 이 문제를 양자물리 문제로 해결해야 한다. 또한 '양자 얽힘' 자체도 양자 상태이므로 이를 이용한 암호 자체가 양자 암호가 된다. 그런데 이 때까지 개발된 많은 알고리즘은 빛의 양을 아주 작은 단일 광자내에서 쓸 수밖에 없다.

예를 들면, 빛의 개수가 2개 이상만 되어도 그 안전성에 심각문제를 초래하게 된다. 양자 암호는 원칙적으로 제3자가 양자 상태인 빛을 건드리기만 해도 데이터의 상태가 바뀌어야 하는데 2개 이상의 광자가 지나가는 동안 공격자는 상대방이 눈치채지 못하도록 하나 이상의 광자를 빼낼 수 있고 그러면 그 가로챈 광자를 이용하여 나중에 어떤 데이터가 오고 갔는지 알 수 있다.

이를 해결하기 위하여 빛을 하나만 쓰는 방법들이 개발되었는데 이는 데이터 송수신에 어려움을 야기한다. 즉 한 개의 광자를 만드는 광원 자체를 만들기도 어렵거니와 이 광자 하나를 측정하는 일도 쉽지 않을 뿐더러 주위의 빛을 차단하고 이 광자의 빛만 골라내는 것도 쉽지 않다. 더구나 단일 광자는 전송 선로상에서 없어지기 쉽기 때문에 실제의 사용에도 문제가 된다. 광자 하나만 만들어 내는 것이 어렵다는 사실을 이용하여 공격자가 이를 공격하기도 한다. 또한 양자 얽힘 상태를 이용하는 방법도 있는데 이는 두 광자가 강하게 서로 연결되어 있어 하나의 상태를 바꾸면 다른 상태도 바뀐다는 양자역학의 기본적인 개념을 이용하는 방법이다. 그러나 이 방법 역시 공격에 취약한 문제점을 노출했다.

이런 문제들을 해결하는 안정된 양자 암호화 방법의 개

발이 양자 암호 연구의 큰 목적 중의 하나이다. 그 중의 하나가 광자 다발을 이용하는 방법인데 이 방법도 아직 제대로 개발되지 못했다. 이유는 이 때까지 개발된 대부분이 양자암호 방법은 하나 이상의 공격에 취약한 문제점을 노출하였기 때문이다. 현재 실험적으로 구현되고 있는 양자암호 방법들도 많은 광자를 이용한 광자다발을 쓰고 있어 실제의 공격에서는 취약하다. 하지만 안정된 양자 암호 방법이 개발되면 실험적 단계는 이미 거친 것이므로 바로 실용화할 수 있게 된다.

양자 암호시스템 상용화 임박

이번에 개발한 양자 암호 방법은 수십 개에 이르는 많은 광자를 이용한 광자 다발을 사용하는 양자 암호화 방법이다. 이렇게 광자가 많아지면 광원이 개발이 쉽고, 송수신에 장애가 발생하지 않으며, 주위 빛과의 구별이 용이하고, 측정이 쉽다는 등의 많은 장점을 가지고 있다. 많은 광자들을 이용할 때 생기는 공격을 어떻게 해결할 것인가인데 이를 위하여 처음 채택한 것이 광자 다발의 편광을 임의의 각도로 매번 변화시키면서 송신하면 양자 역학의 한계 때문에 광자 다발의 편광을 정확히 측정하지 못한다는 것이다.

두 번째로 채택한 방법은 두 광자 다발을 동시에 사용하고 마지막 정보를 송신할 때 그 중 하나를 취하고 하나를 버림으로써 어느 광자 다발을 취했는지 모르게 하는 것이다. 물론 이 중간에 광자 다발들의 편광 각도를 변화시켜 제3자가 이를 알지 못하도록 감추는 방법이 포함되어 있다. 이런 방법을 사용하면 제 삼자는 광자 다발을 취하여 편광 상태를 측정하기 위해서는 양자 역학의 한계에 봉착하게 되고 그 한계로 인하여 제3자가 개입하면 광자 다발이 상태가 바뀌어 송수신자는 제3자의 개입을 파악할 수 있는 것이다. 이 방법을 이용하면 현재 암호방법에서 패스워드에 해당하는 비밀키 값을 안전하게 보낼 수 있게 된다. 이 방법은 매우 실용적인 방법으로 실제 양자 암호에 그대로 사용할 수 있다. 그 방법은 광통신 선로를 이용할 수도 있고, 공중으로 빛을 보낼 수도 있다. 현재 세계적으로 적용된 실험들은 양자 암호를 사용함에 있어 아직 기술적인 한계 때문에 단일 광자를 쓰지 못하고 광자 다발을 쓰는데 수백 개의 광자들이 모인 광자 다발을 이용하여 양자 암호를 실행한다.

그 예로 영국의 브리스틀 대학과 미국의 로스알라모스 연구소는 대낮에 10~20㎞에 이른 거리의 양자 암호에 성공했다. 이는 낮이라는 조건에서 태양광이 강한 광자를 만듦에도 불구하고 이를 적절히 제어할 수 있었기 때문이다. 2003년 일본의 도시바는 100㎞의 거리를 광통신망을 이용하여 성공적으로 정보전달에 성공하였고, 2004년 6월에는 미국의 매사추세츠주의 케임브리지시에 소재한 BBN 테크놀로지와 하버드 대학 사이의 10㎞ 거리의 양자 통신망을 건설했다. 또 2004년 4월에는 오스트리아 빈에서 양자 암호기술이 적용된 은행 송금 시스템을 통해 성공적으로 송금을 했다. 이런 일련의 실험적 사실은 양자 암호기술이 먼 미래의 일이 아니라 곧 다가올 새로운 기술이라는 것을 말해 준다.

선진국보다 앞선 기술보유 멀지 않아

양자 암호기술이 개발되면 선진국에서는 도청이 불가능한 암호시스템을 상용화해 쓰겠지만 이런 기술이 적용되지 못하는 나라는 정보가 그대로 노출되는 결과를 초래하게 된다. 최근 국내에서도 이에 대한 중요성을 인식하여 소수의 물리학자들이 이에 대한 연구를 지속하고 있다. 우리 연구단의 연구결과는 이 때까지 개발된 방법 중 안정성이 확보된 실용화에 가장 가까운 양자 암호 방법으로 평가받고 있으며 앞으로 이 성과물을 상용화에 적용하는 과제를 남겨두고 있다. 좀 더 우수한 양자 암호 방법의 개발과 그 개발된 기술을 보완하는 것, 그리고 이 방법을 새로운 암호체계에 적용하는 방법을 개발하는 것이 중요한 과제이다. 아울러 양자 암호를 실험실 수준에서라도 성공시키는 일 역시 빼놓을 수 없는 숙제다. 이런 일련의 일들이 성공적으로 수행되면 우리 나라가 선진 외국의 결과보다 훨씬 좋은 양자 암호방법을 확보할 수 있게 된다. 이를 위해서는 국내 다른 학자들의 도움 뿐 아니라 더 나은 개발기술 여건을 위한 투자 역시 선행되어야 할 것이다. ST

글쓴이는 서강대 물리학과를 졸업한 후 동 대학에서 석·박사학위를 받았으며, 미국 센트럴플로리다 대학에서 연구원으로 재직했다.