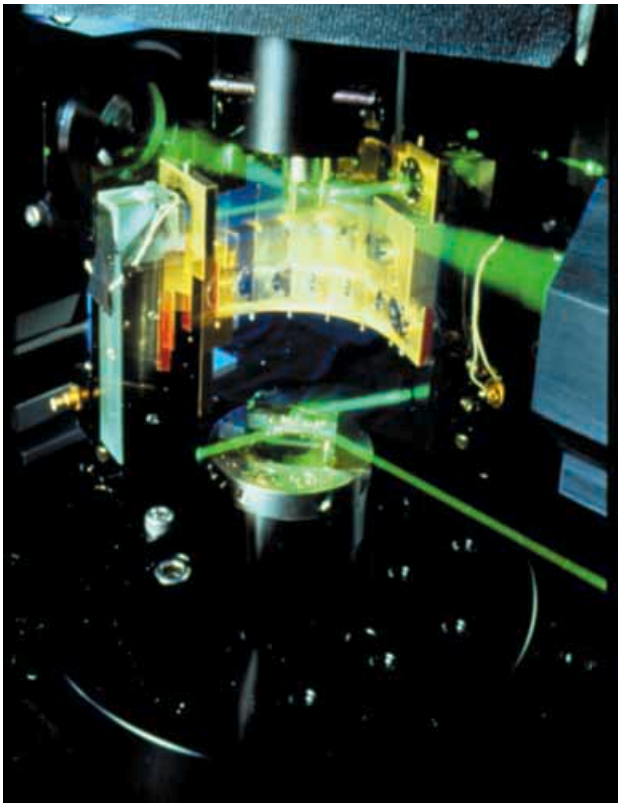
도청·복사 불가, '양자 암호' 시대 온다

글 _ 박방주 중앙일보 과학전문기자 bpark@joongang.co.kr

빛은 광자가 다발로 쏟아지는 현상이다. 전자가 전기를 옮기듯 광자도 빛을 전파하는 것이다. 형광등 하나가 내뿜는 광자는 셀 수 없을 정도로 많다. 그 빛을 계속 어둡게 해나가다 보면 언젠가는 한 개의 광자만 남을 수 있다. 그 광자 하나하나에 암호를 실어 보낸다면 어떨까. 그 누구도 도청하지 못하는 무적의 암호가 된다. 이른바 양자암호다.

기존 공개키 암호는 언젠가는 풀 수 있어

양자암호가 1984년 IBM 찰스 베넷 박사와 몬트리올대의 브라사드 교수에 의해 개발된지 올해로 20년이 됐다. 양자 암호에 대한 이론이 처음 나올 당시만 해도 신기한 하나의 과학 이론 정도로만 받아들여졌다. 이를테면 도저히 실현할 수 없는 하나의 신기루라고 보는 분위기였다는 것이다. 베넷 박사는 이론 물리학자임에도 불구하고 실험 장치를 직접 제작했다. 자신의 이론을 증명해보이고 싶었던 것이다. 결국 1989년 세계 최초의 양자암호 실험을 성공하기에 이르렀다. 그러나 그 역시 암호 세계에 큰 인상을 주지 못했다. 기존의 공개키 암호가 워낙 탄탄했으며, 암호 세계에 미치는 영향력이 컸기 때문이다. 더구나 공개키 암호는 언제까지라도 풀리지 않을 것으로 믿고 있었던 영향도 있다.

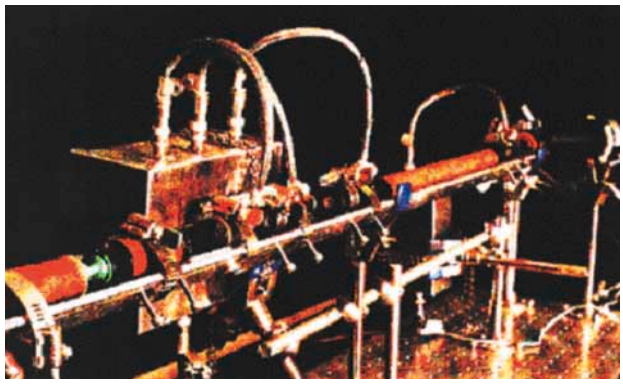


공개키 암호는 현재 인터넷, 통신장비 등에서 주요 암호로 사용되고 있는 것이다. 이를 처음 개발했던 리베스트, 샤미르, 에이들먼 등 세 사람은 큰 돈을 벌고 있다. 이들 이름의 첫글자를 따 공개키 암호는 'RSA 암호키' 라고도 한다.

공개키 암호 기술은 큰 수의 소인수분해를 이용한다. 수십 자리에 해당하는 소수 두 개를 곱해 만든 아주 큰 자연수가 공개키가 되는 것이다. 이 수가 암호를 푸는 열쇠인 셈이다. 공개키 암호에 사용하는 이런 열쇠를 찾으려면 지금 가동중인 최고 성능의 컴퓨터로도 수백 년을 풀어야 한다. 그러니 공개키를 필적할만한 어떤 암호시스템이 나올 것으로 생각하는 사람들은 많지 않았으며, 양자 암호 역시 눈길을 끌지 못한 것이다.

공개키에 대한 자신감을 읽을 수 있는 일화도 있다. 공개키 개발자들은 1977년 미국의 대중 과학잡지인 '사이언티픽 아메리칸' 에 자신들이 만든 129자릿수의 자연수를 소인수 분해하는 사람한테 100달러를 주겠다는 현상을 걸었다. 개발자 중의 한 사람은 1초에 10억 번을 계산하는 컴퓨터를 쓰더라도 4경(京)년이 걸릴 것으로 내다봤다. 그런 컴퓨터는 실제 1990년대에 나왔다. 그러나 1994년 4월2일 이 문제가 풀렸다. 전세계 25개국 600여 명의 동호인들이 1천600여 대의 컴퓨터를 네트워크로 연결해 병렬 계산을 하기 시작했다. 그런 뒤 8개월 만에 해답을 얻어낸 것이다. 이는 공개키 암호시스템이 어렵기는 해도 시간이 문제일 뿐 언젠가는 풀린다는 것을 역설적으로 알려준 사건이었다.

무선으로 광자를 쏘아 양자암호를 송수신하는 장치. 망원경처럼 생긴 곳으로 광자 날개가 튀어나가거나 받는다.



IBM의 첫 양자암호 전송장치

원본 손대면 정보 변형, 복사 · 도청 원천 차단

양자 암호는 시간이 아무리 흘러도 열쇠가 없으면 풀 수 없다. 그렇지만 그런 우수성에도 불구하고 개발된 이후 그 동안 연구실 차원에서나 다뤄졌다. 그러다 최근 들어 양자암호는 비약적인 발전을 보고 있다. 본격적으로 실용화되고 있는 것이다.

지난 4월 오스트리아 빈 시장은 세계 처음으로 양자암호기술이 적용된 은행송금시스템으로 빈대학의 차일링거 교수의 계좌에 3천유로를 송금했다. 지난 6월 미 매사추세츠주 케임브리지시의 BBN테크놀로지와 하버드대 사이 10㎞ 거리에 양자통신망이 설치됐다. 지난해에는 일본 도시바가 100㎞ 거리의 광섬유로 양자암호통신을 성공하기도 했으며, 스위스의 한 업체는 양자암호통신장치를 판매하고 있기도 하다.

단일 광자 전송은 베넷 박사가 처음 실험에 성공할 당시에는 32㎝를 전송했다. 지금은 최대 120㎞까지 길어졌으며, 네트워크도 어느 정도 구축할 수 있다는 것을 확인했다. 즉, 일대일 통신이 아니라 여러 사람을 서로 연결해 원하는 사람에게 양자를 전송할 수 있게 됐다는 것이다. 양자암호가 무적의 암호시스템으로 떠오르는 이유는 무엇일까.

고등과학원 계산과학부 김재완 교수는 "기존 암호시스템은 시간이 좀 걸려서 그렇지 언젠가는 풀리게 된다"며 "양자암호는 도청하거나 복사하지 못하는 완벽한 암호"라고 말했다. 암호를 저장하고 있는 양자는 중간에 다른 사람이 복사하면 복사하는 순간 양자에 저장된 정보가 달라지는 데다 원상태로 되돌릴 수 없다. 인터넷에 있는 정보는 내려받아도 원본에는 전혀 변화가 없는 것과는 완전히 다르다. 이 때문에 양자를 누군가 중간에 복사 또는 도청하면 즉시 들통 난다.

인터넷 통신을 비롯한 군 통신 등에는 거의 대부분 암호를 섞어 주고 받는다. 이를테면 원문에 송수신하는 사람만 아는 숫자를 더하거나 빼서 보낸다. 수신자는 수신한 정보에서 암호 숫자를 없애면 알맹이 정보만 남는 식이다.

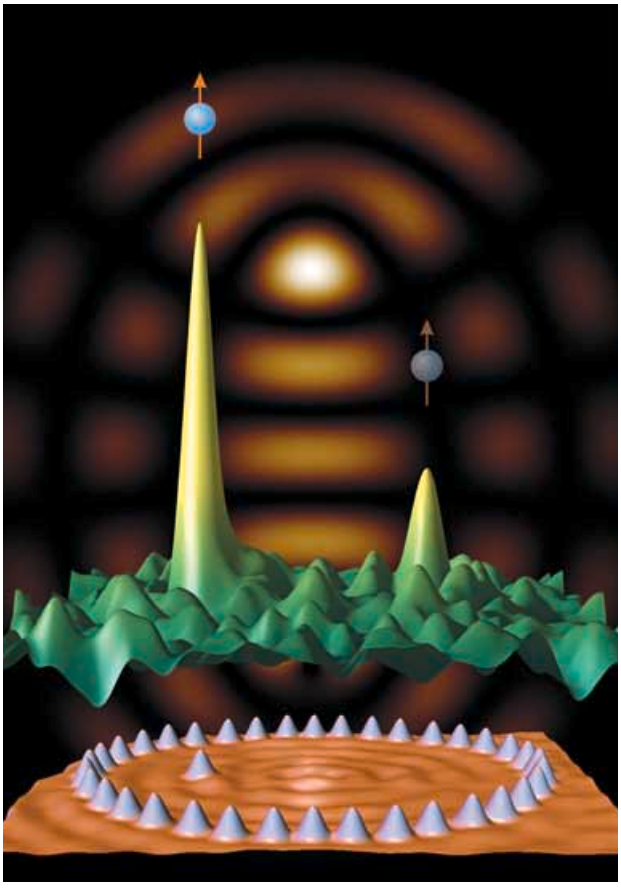
현재 양자암호가 상용화된 것은 광섬유를 이용한 광통신에서다. 광섬유에 낱개 광자를 연속해 쏘아 수신처에 도달하게 하는 것이다. 이는 광섬유가 광자를 흡수하지 않고 잘 전달하기만 하면 됐다. 중간에 장애물이 없기 때문이다. 그러나 최근 들어 무선으로 양자암호통신을 시도해 성공해 양자암호의 응용 가능성을 크게 넓히고 있다.

미국 · 영국 · 일본 등서 무선 암호통신 성공

영국 브리스틀대, 미국 로스앨러모스연구소팀은 각각 햇빛이 내려쬐는 대낮에 10~20㎞의 양자암호 통신에 성공했다. 이는 대낮에는 태양에서 쏟아지는 광자가 암호를 실은 광자와 섞이거나 태양의 활발한 활동으로 인해 원래의 신호가 변질될 수 있어 매우 어려운 실험이다. 또 광자를 정확하게 상대방에게 겨냥하지 않으면 엉뚱한 곳으로 날아갈 우려도 있다. 이 실험의 성공은 위성통신에 양자암호를 사용할 수 있는 길을 열었다는 평가를 받고 있다.

양자암호가 기존 암호시스템과 다른 점은 양자가 갖는 특성 때문이다. 양자는 광자나 이온 · 원자핵 등으로 만들 수 있다. 반도체칩에서는 0이나 1 중 어느 하나만을 한 비트에 저장하지만 양자에는 0과 1 외에 두 가지가 중첩되어 있는 상태도 저장할 수 있다. 즉, 이에 따라 8개의 한 바이트에는 윷놀이할 때 나타나는 도 · 개 · 걸 · 윷의 16가지 조합을 동시에 나타낼 수 있

베넷 박사가 고등과학원에서 양자암호에 대해 강의하는 모습



금속의 원자를 특수현미경으로 본 모습

다. 기존 반도체는 어느 한 가지만을 표시할 수 있을 뿐이다.

양자를 연속적으로 발생시키는 실험도 성공했다. 일본 정보통신연구기구 간사이첨단연구센터의 하야사카 가즈히로 주임연구원과 독일 막스프랑크 양자광학연구소는 지난 11월초 이온 트랩 공진기로 시간 파형과 타이밍을 고정밀도로 제어한 단일 광자를 발생시키는데 처음으로 성공했다. 연구 성과는 '네이처'에 발표됐다. 연구팀은 90분 동안 6만 발의 단일 광자를 연속적으로 발생시켰으며, 양자중첩 현상도 관측했다. 이런 결과는 양자 네트워크를 구성하는 것이 가능하게 된다. 지금까지는 네트워크 구축이 대단히 어려웠다. 또 양자를 중계할 수 있어 암호통신의 거리를 늘릴 수 있게 된다. 이는 양자 암호의 본격적인 실용화에 결정적인 역할을 할 것으로 기대되는 것이다. 양자 중계는 지금까지는 불가능한 것으로 여겨졌다. 양자를 중계한다는 것은 중간에 양자를 복사하거나 만지는 과정이 필수적이다. 그러나 양자는 만지는 순간 그 상태가 변해버리는 성질을 가지고 있다. 이 때문에 중계가 불가능했다. 이번 연구 성과는 이런 점에서도 대단히 혁신적이다. 아직 양자암호는 풀어야 할 숙제도 많다. 지금은 양자를 복사하거나 증폭시킬 수 없다. 그렇게 하면 당장 양자상태가 변해버리기 때문이다. 현재까지 성공한 실험이나 상용제품도 어느 두 지점간에만 송수신이 된다. 이 때문에 태평양을 횡단하는 것은 고사하고, 대도시 안에서도 양자암호장치를 사용하는 데 한계가 있다.

양자 암호가 실용화되는 것에 맞춰 세계 암호계는 양자 암호를 새로운 패러다임으로 받아들이고 있다. 공개키 암호 시대는 가고 양자암호 시대가 화려하게 등장할 것으로 보는 것이다. 이에 따라 미국, 일본 등 선진국은 양자암호 연구에 대규모 투자를 하는 등 각별한 관심을 기울이고 있다. 일본만 해도 양자 관련 국제 학회가 매년 두세 번 열리고 있을 정도다. 전세계적으로 연간 5천만 달러 규모의 양자암호 연구가 진행되고 있는 것으로 추산되고 있다. 그러나 우리나라는 전문가도 서너명에 불과하며, 정부의 투자는 극히 미미한 수준이다. 김 교수는 "양자암호 장치는 지금 극히 초보적인 상태지만 얼마 안가 지금의 암호장치를 대체할 것"이라며 "우리나라도 이 분야의 연구개발에 적극 나서야 한다"고 말했다. ST

글쓴이는 경희대 전자과를 졸업 후, 동대학원에서 석사학위를 받았다.