진정한 무작위가 가능할까?
양자난수생성기

김재완 고등과학원 교수

최근 한 국내 기업이 스마트폰에 양자난수칩을 내장하여 통신보안을 강화하였다는 보도가 있었다. 마구잡이수 또는 막수라고도 불리는 난수(亂數, Random number)는 보안이나 컴퓨터 시뮬레이션 같은 정보처리에 매우 중요한 자원이다. 예컨대 보안에 필요한 비밀번호를 아무나 쉽게 추측할 수 있고 열람도 가능하다면 소용이 없을 것이다. 따라서 보안에는 누구도 예측할 수 없는 수, 난수를 사용한다. 양자난수생성기는 난수생성에 양자현상을 이용해 통신보안을 한층 강화하는 기술이다.

공개키 암호와 양자컴퓨터

통신보안에서는 두 통신 당사자 사이에 어떤 식으로 메시지를 암호화할지 합의해야 한다. 우선 공개키암호방식이 있다. 수신자가 공개한 키를 이용해 송신자가 암호화하여 보내는 방식이다. 수신자가 송신자와 비밀 자물쇠 번호를 공유하는 셈이다. 이렇게 한번 암호화된 메시지는 열쇠에 해당하는 비밀키로만 해독할 수 있다. 당연히 자물쇠와 열쇠는 서로 관련이 있지만, 자물쇠를 알더라도 열쇠를 추측하는 것은 매우 어렵게 설계되어 있다.

자물쇠와 열쇠가 서로 다르기 때문에 비대칭 암호라고도 하는데, 그 대표적인 RSA 방식은 큰 수를 소인수분해하는 방식을 사용한다. 그런데 양자컴퓨터가 등장하면 소인수분해는 쉬운 문제로 전락하고 말 터라 미국 국가안보국(NSA)은 현재의 암호체계를 대체할 기술이 필요하다고 권고한 바 있다. 양자컴퓨터로도 못 풀 포스트양자암호(Post-quantum cryptography)나 양자암호가 대안이 될 수 있을 것이다.

일회용 난수표와 양자암호

안전한 암호통신 방식 중 일회용 난수표 방식이 있다. 두 통신 당사자가 똑같은 난수를 비밀키로 나눠 가지므로 대칭형 암호에 속한다. 갑이 을에게 보낼 메시지를 숫자로 바꾸고 여기에 난수를 더해서 만들어진 암호문을 을에게 보낸다. 을은 암호문에서 난수를 빼고 이 숫자를 원래의 메시지로 복원한다. 이런 과정을 모두 이진수 비트로 하는데, 같은 두 비트를 더하거나 빼면 0, 다른 두 비트를 더하거나 빼면 1이 된다. 동일한 난수를 두 번 이상 사용하면 간단한 연산을 거

쳐 키를 추측할 수 있으므로 메시지를 보낼 때마다 새로운 난수를 생성해 사용함으로써 보안 문제를 해결한다.

이외에도 난수를 공개키 암호 방식으로 보내는 방법도 있고, 일단 한 번 나눠 가진 난수로 메시지를 여러 번 반복하여 자르고 섞는 해시(hash) 과정을 쓰는 DES나 AES와 같은 대칭암호방식도 있다. 그러나 양자컴퓨터가 등장하면 이런 방식들이 모두 안전하지 않게 된다.

양자암호는 갑과 을이 양자물리학적인 과정을 이용하여 양쪽에 똑같은 난수를 만들어 이를 비밀키로 이용하는 것이다. 갑이 을에게 단일광자를 보내는 BB84 방식은 갑이 보내고 을이 측정하는 양자코딩 방식과 다르면 같은 비트를 공유할 확률이 50%이므로 버리고, 방식과 같으면 같은 비트를 얻으므로 이 비트들을 모아서 일회용 난수로 공유한다. 양자얽힘을 이용하는 E91 방식은 서로 얽히는 양쪽의 측정결과를 난수로 공유한다.

유사난수, 진짜난수, 양자난수

양자물리학을 이용하여 둘이서 함께 난수를 만들어 공유하는 것이 양자암호라면, 양자난수생성은 혼자서 난수를 만들어 보안에 사용하는 것이다. 그렇다면 양자난수는 기존의 난수와 어떤 점이 다르기에 보안성이 높은 걸까? 현재 흔히 보안에 사용하는 난수는 '유사난수'다. 유사난수(PRN, Pseudo-Random Number)는 수학적인 알고리듬을 사용하여 결정론적인 과정으로 만든다. 그렇기에 컴퓨터를 사용하여 많은 수를 순차적으로 대입하는(brute force) 공격에 취약하다.

이에 비해 예측이 불가능하거나 어려운 데이터를 수집하는 엔트로피 수집(entropy gathering)으로 만드는 난수를 물리적 난수(physical random number) 또는 진짜난수(TRN, True Random Number)라고 한다. 양자난수(QRN, Quantum Random Number)는 비결정론적인 양자측정(Quantum measurement)을 이용하는 진짜난수의 일종이다.

양자물리학의 측정은 확률에 따르는 과정이므로, 어떤 특정 결과가 나올지 예측하는 것은 불가능하고 오로지 확률만 알 수 있다. 물리적인 무작위성이 나타나는 셈이다. 따라서 양자측정의 결과를 숫자에 대응시키면 예측이 불가능한 완전한 난수를 물리적으로 생성할 수 있다.

양자난수를 만들 수 있는 다양한 양자물리현상 중에 가장 오래된 방법은, 방사성원소의 붕괴를 이용하는 것이다. 방사성원소의 붕괴 과정은 포아송 분포를 나타내는 확률과정으로, 1950년대부터 가이거계수기로 알파입자를 검측하여 이를 난수로 활용하고자 채집하여 이용해 왔다.

단일광자를 이용한 양자광학적 방법으로는, 수평편광과 수직편광 상태가 중첩(Superposition)된 45도 편광 단일광자를 편광분할기에 통과시키면 수평으로 나올지 수직으로 나올지 예측이 불가능하므로 이를 양자난수생성기로 쓸 수 있다.

최근 보도된 양자난수칩은 단일광자가 아닌 레이저광을 이용한다고 한다. 레이저 광은 광자의 개수가 0, 1, 2, 3, … 등인 여러 상태의 중첩이다. 광자 몇 개의 상태가 측정되느냐 하는 것은 예측이 불가능한데, 이번에 스마트폰에 내장된 양자난수생성기는 이 확률과정에서 난수를 채집하는 방식이다.

양자난수생성은 양자암호는 아니지만 유사난수나 진짜난수에 비해 훨씬 나은 통신보안을 제공한다. 양자난수를 통신당사자들끼리 나눠가지는 것은 여전히 RSA나 AES와 같은 고전적인 암호방식을 사용하겠지만, 양자암호나 포스트양자암호 등으로 훨씬 강화될 것으로 기대된다.