새로운 형식의 보안 -양자

윤춘석 (주)KT 융합기술원 선임연구원

1. 머리말

암호의 역사는 상당히 오래되었다[1]. 역사상 가장 오래된 암호의 기록은 기원전 400년경 고대 그리스인들이 쓰던 스키테일 암호다. 스키테일 암호는 굵은 원통형 막대에 가느다란 종이를 감아 보내고자 하는 메시지를 적고, 남은 부분을 의미 없는 글자들로 채워서 보내는 것이다. 메시지를 확인하려면 처음 메시지를 작성할 때 사용한 원통 막대와 같은 굵기의 막대에 다시 종이를 감아 글자들을 읽어내면 된다.

[그림 1] 스키테일 암호 사진[2]

현대의 시각에서 보면 특정 글자 갯수로 묶은 블록당 한 글자씩만 읽으면 되기 때문에 매우 간단하게 풀 수 있지만, 암호의 개념이 없던 옛날에는 꽤나 획기적인 방법이었을 것이다.

이렇듯 인류는 오랜 옛날부터 비밀스러운 무언가를 전달하는 방법을 만들어왔다. 전쟁의 통신용, 특정 그룹의 소속감과 유대감을 확보하려는 수단, 연인에게 사랑을 전하는 방법 등의 목적을 위해 방법들을 발전시켜 왔다.

오랜 시간이 흘러, 수학의 발전과 기계의 사용은 암호학의 새로운 도약을 가져왔다. 사람이 손으로 암호화를 수행하던 것에서 벗어나서 기계를 통한 암호 시스템을 만들게 된다. 현대 암호의 시작이다.

현대 정보이론의 아버지로 불리는 섀넌(Claud Elwood Shannon)은 1945년 Bell랩에 <A Mathematical Theory of Cryptography, 1945>라는 보고서를 제출한다.(이 보고서는 1949년 기밀이 해제되어 <Communication Theory of Secrecy Systems, 1949>라는 이름으로 발표된다) 섀넌은 이 보고서에서 일회성 암호 체계가 안전함을 증명하고, 동시에 혼돈과 확산 이론을 제시한다. 이 이론을 토대로 발달한 것이 대칭키 암호 시스템(Symmetric-key Cryptography)이다.

대칭키 암호 시스템은 암호화/복호화에 동일한 키가 사용되는 암호 시스템이다. 내부 구조가 간단해 연산 속도가 빠르다는 장점을 가진다. 하지만 송수신자가 동일한 키를 공유해야 하는 특성상 정보를 주고받는 대상이 늘어날 경우 키의 수가 대상 수만큼 늘어남에 따라 저장 및 관리에 어려움이 생긴다.

한편, 1976년 스탠퍼드대학교의 디피(Whitfield Diffie)와 헬만(Martin Hellman)은 <New Directions in Cryptography>라는 논문에서 처음으로 공개키 암호 시스템의 개념을 제안한다. 이는 불특정 다수 사용자 간에 사전에 키를 나눠가지는 단계를 생략한 채 보안 통신을 하는 방법을 제공했다.(공개키 암호 시스템의 암복호화 순서를 역으로 활용하면 전자서명 기능도 제공할 수 있다) 다만, 이를 구현하기 위해서는 복잡한 수학문제를 활용하기 때문에 대칭키 암호 시스템에 비해 연산 속도가 느리다.

현대의 보안통신은 앞 두 가지 암호 시스템을 적절히 활용한 하이브리드 타입도 사용한다. 공개키 암호 시스템을 이용해 암호통신을 위한 대칭키를 나눠가진 후, 대칭키 암호 시스템을 이용해 대용량 암호 통신을 수행하는 것이다. 이는 사전에 키를 나눠가지지 않으면서도 빠른 암호통신을 가능하게 해주는 장점을 가진다.

하지만 1980년대 리처드 파인만(Richard Phillips Feynman)은 이런 현대 암호시스템에 큰 파장을 불러일으킬 한 컴퓨터의 등장을 예고한다. 그리고 2019년 구글은 시커모어라는 이름의 프로세서를 장착한 양자컴퓨터를 선보인다. 시커모어는 양자 우월성(Quantum supremacy)을 최초로 달성한 양자컴퓨터이다.

이는 현대 암호학이 더 이상 안전하지 않을 수 있음을 말하며, 새로운 암호시스템을 찾아야 할 필요성을 제기한다.

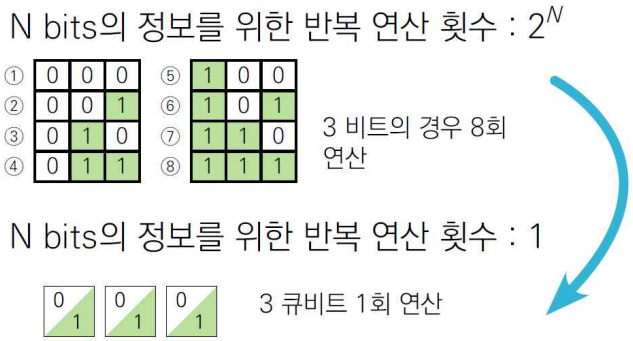
2. 양자컴퓨터와 새로운 보안 위협

2.1 양자컴퓨터란?

현대의 컴퓨터는 정보를 처리하기 위해 비트(Bit) 단위를 사용한다. 각 비트는 0 또는 1로 표현되며, 이 비트들의 조합으로 정보를 만들고 저장하고 처리하는 연산을 수행한다. 이것이 현재 우리가 쓰는 컴퓨터다.

양자컴퓨터는 정보를 처리하기 위해 큐비트(Qubit, Quantum Bit)를 사용한다. 각 큐비트는 0과 1이 동시에 존재하는 중첩(superposition), 여러 개의 큐비트가 서로 강력한 상관관계를 가지는 양자 얽힘(entanglement) 같은 물리적 현상을 활용하여 정보를 처리하는 컴퓨터다. 위 현상을 활용하는 양자컴퓨터는 각 경우의 수에 해당하는 정보를 동시에 처리할 수 있어 연산 속도가 기존 컴퓨터에 비해 매우 빠른 것이 특징이다.

예를 들어 2비트 정보를 처리한다고 가정하면, 현대의 컴퓨터는 00, 01, 10, 11의 4가지 경우에 대해 4번에 걸쳐 연산을 수행해야 한다. 하지만 양자컴퓨터는 4가지 경우가 중첩되어 있는 2큐비트를 활용하여 동시에 연산을 수행할 수 있다. 이를 확장하여 n비트 정보를 처리할 경우 엄청난 속도의 향상을 기대할 수 있다.



[그림 2] 일반 컴퓨터(위)와 양자컴퓨터의 연산 원리 비교

물론 큐비트의 측정이 확률적으로 이루어지므로 무조건 1번의 연산으로 모든 경우에 대한 연산 결과를 알 수 있는 것은 아니다. 의미 있는 상태가 나타날 확률을 높이기 위한 추가 작업이 필요하기도 하고, 양자 얽힘 상태를 만들거나 오류보정을 위한 추가 비용이 발생하는 단점도 있다.

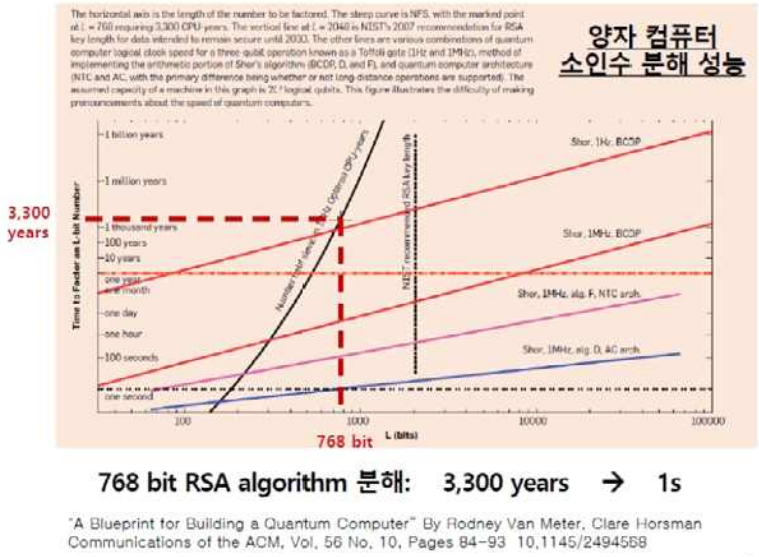
그럼에도 불구하고, 입자의 양자적 특성을 활용하여 정보를 표현하고 연산을 수행하는 실험들이 수행되면서 양자컴퓨터를 만들 수 있는 희망이 생겼다. 앞서 말한 단점들을 극복하기 위한 다양한 방법들도 연구되고 있다. 현재 D-wave, 구글, IBM, 아이온큐 등 다양한 기업들이 양자컴퓨터 상용화를 위해 연구하고 있는 만큼 가까운 미래에 상용 양자컴퓨터를 볼 수 있게 될 것이다.

2.2 공격받은 RSA

공개키 암호 시스템의 대표주자인 RSA는 1978년 MIT의 로널드 라이베스트(Ron Rivest), 아디 샤미르(Adi Shamir), 레너드 애들먼(Leonard Adleman)에 의해 만들어졌다.(3명의 발명자의 이름을 따 RSA라고 부른다. 1997년 발표된 내용에 따르면, 비밀로 취급되어 공개되지는 않았으나 1973년 영국에서 먼저 개발했다는 내용도 있다) RSA는 현재 가장 널리 쓰이고 있는 공개키 암호화 알고리즘일 뿐만 아니라, 전자서명/인증이 가능한 최초의 알고리즘으로도 알려져 있다. 이에 따라 전자 상거래 등에도 광범위하게 활용되고 있다[3].

RSA는 큰 수의 소인수 분해는 어렵다는 수학적 알고리즘에 기반한 암호 알고리즘이다. 현재 RSA 알고리즘을 사용하는 시스템에서는 1024비트 또는 2048비트 크기의 수를 사용하는데, 이 수를 소인수 분해 하려면 우주의 나이보다 긴 시간이 필요하다[4].(접근 방법에 따라 약간의 차이는 있을 수 있다) 이는 암호 시스템을 공격해서 얻어내는 정보의 가치가 무한하지 않다면 의미가 없는 공격이 된다.

그런데 쇼어(Peter Shor)가 1994년 발표한 논문에서 쇼어 알고리즘(Shor's algorithm)이라는 것을 제안한다[5]. 쇼어 알고리즘은 양자컴퓨터가 있을 때, 소인수 분해 문제에 현재까지 알려진 알고리즘에 비해 지수레벨의 속도 향상을 가져오는 알고리즘이다. 이 알고리즘을 사용하면 768비트 크기의 수를 소인수 분해하는 데 약 1초의 시간이 소요된다[4]. 현존하는 가장 널리 사용되는 공개키 암호 시스템이 더 이상 안전을 보장할 수 없게 된다. 또한, 이산로그 문제도 공격을 받기 때문에 엘가말이나 타원곡선 암호의 일부도 더 이상 안전하다고 볼 수 없다.



[그림 3] 양자컴퓨터의 소인수 분해 성능[4]

1996년 그로버(Lov K. Grover)는 Database에서의 정보의 탐색과 관련, 현대 컴퓨터에서는 지수적인 시간 복잡도에서 해결할 수 있는 문제를 다항 시간 안에 풀 수 있도록 한 양자컴퓨터용 알고리즘을 제안했다[6][7]. 그로버 알고리즘은 정렬되지 않은 데이터베이스에서 특정 정보를 찾는 속도를 비약적으로 향상시켰다.

이 알고리즘은 쇼어 알고리즘과는 다른 암호시스템을 공격했는데, 대칭키 암호 알고리즘의 비밀키 사이즈와 해시 알고리즘의 출력 사이즈를 각각 2배, 3배 증가시켜야만 기존과 동일한 안전성을 확보할 수 있다.

만약, 적절한 대응책을 마련하기 전에 양자컴퓨터가 상용화된다면 현대의 암호 시스템은 더이상 정보를 보호할 수 없으며, 현대 정보 자산은 치명적 타격을 입게 될 것이다.

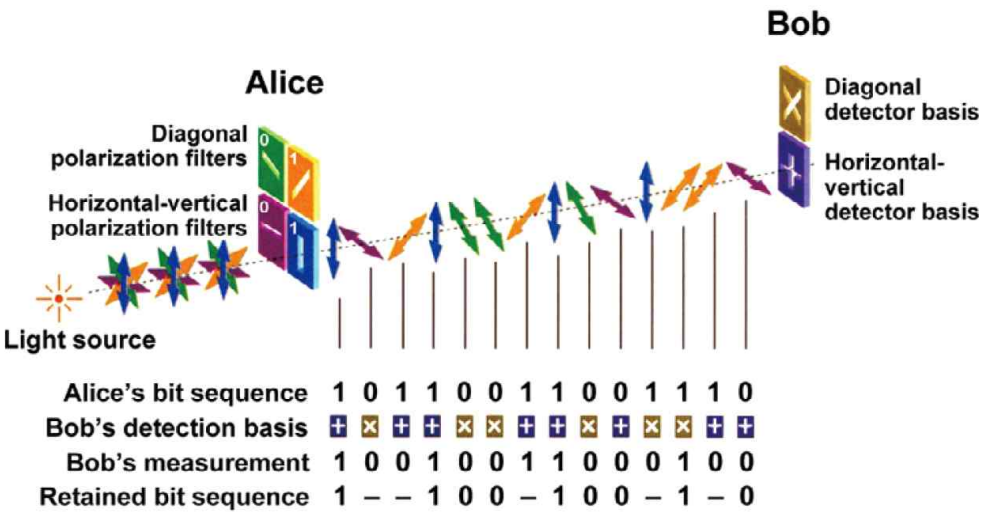
2.3 대응하는 두개의 움직임

2.3.1 양자암호

양자암호란 양자역학적 성질을 활용한 암호시스템이다. 양자암호는 수학적 복잡성에 기반을 두지 않고 물리적인 성질에 기반하고 있기에, 연산 속도의 문제로 공격받을 염려를 하지 않아도 된다. 이는 양자 암호 시스템을 공격하기 위한 효율적인 수학적 알고리즘이 개발될 수 없으며, 더 빠른 컴퓨터가 미래에 개발된다고 하더라도 안전한 암호시스템을 만들 수 있음을 의미한다.

가장 대표적인 것은 양자 키 분배(QKD, Quantum Key Distribution) 프로토콜이다. 현대 보안통신시스템에서 사용하는 공개키 암호 알고리즘을 활용하여 대칭키를 나눠 가지는 부분을, 양자적 성질을 활용한 키 분배 프로토콜로 대체하는 방법이다. 이렇게 나눠 가진 암호키를 활용하여 대칭키 암호 알고리즘을 사용한 암호통신을 하게 된다.

대표적인 양자 키 분배 프로토콜로는 BB84가 있다[8]. 베넷(Charles Bennett)과 브라사드(Gilles Brassard)가 1984년 발표한 첫 번째 양자 암호 프로토콜이다. BB84는 양자키 분배 기술 중 이론적으로 안전성이 가장 잘 증명되어 있으며, 가장 많이 구현되고 있는 프로토콜이다.



[그림 4] BB84 프로토콜의 구조

BB84 프로토콜을 쓰면 비밀키를 큐비트를 통해 송수신하는 과정에서 공격자가 도청을 시도하더라도 발각될 수밖에 없다. 전송 중인 큐빗은 공격자가 도청하기 위해 측정하는 순간 기존의 물리적 성질을 잃어버리게 된다. 또 송신자의 송신 편광을 알 수 없는 공격자는 자기가 측정한 정보를 토대로 예측한 큐빗을 보내게 되고, 정당한 수신자는 공격자가 다시 보내준 큐빗을 받게 될 경우 후처리 과정을 통해서 중간에 공격자의 개입을 알 수 있게 된다. 이때 공격자를 발견하게 될 확률은 다음과 같다.(단, n은 주고받은 큐비트 수) n이 수십 큐비트만 되어도 공격자가발견될 확률은 거의 100%이다.

양자 키 분배 시스템은 세계적으로 가장 활발하게 개발되어 실증 사업이 추진되고 있는 양자암호 분야이다. 미국, 유럽, 중국, 일본, 한국 등 세계 각국이 관심을 가지고 시범 사업 등을 추진하여 상용화에 박차를 가하고 있다.

RSA가 양자컴퓨터에 의해 공격받음으로 인해 대체해야 하는 암호 시스템은 키 분배 프로토콜 뿐만 아니다. 인증/서명 알고리즘도 대체되어야만 한다. 양자암호 분야에도 역시 양자인증/양자서명과 같은 알고리즘들도 연구되고 있다. 다만, 전송과 검출 기술 구현의 한계로 인해 아직 실험실에서 연구하는 수준이다.

2.3.2 양자내성암호(PQC, Post Quantum Cryptography)

양자내성암호는 수학적 어려움을 기반으로 한다는 점에서 현대 암호학과 결을 같이한다. 다만, 양자컴퓨터를 통해 공격받지 않은 다른 수학적 복잡성에 기반한 문제들을 활용하기 때문에 안전성을 보장받는다. 격자(Lattice), 코드(Code), 다변수(Multi-variate), 해시(Hash), 아이소제니(Isogeny)를 기반으로 하는 5가지 방식이 현재 가장 유력한 양자내성 암호로 연구되고 있다. 각 알고리즘들은 양자컴퓨터에 공격받은 공개키 암호 시스템을 대체하기 위하여 암호 알고리즘뿐만 아니라 인증/서명 알고리즘으로도 개발되고 있다.

각각의 방식은 특성에 따라 여러 장단점을 가지며, 세계 각국에서 효율적이면서 안전한 양자내성암호를 만들기 위해 여러 연구를 하고 있다. 특히 미국 NIST는 양자내성암호 표준을 선정하기 위한 절차를 진행하는 중이다[9].(엄밀히 말하면 양자내성암호는 양자역학적 성질을 활

용한 기술이 아니므로, 본문에서는 구체적으로 설명하지 않는다)

2.4 관련 표준화 이슈 및 현황

양자암호 기술 관련 국제 표준화 움직임은 크게 3가지로 나뉘어 볼 수 있다.

2.4.1 유럽전기통신표준협회(ETSI)

ETSI는 2010년부터 양자 키 분배 기술 관련 다양한 표준들을 개발하고 있다. 용어, 구성요소, 프로토콜, 안전성 증명, 인터페이스 등 주로 양자키 분배 장비에 특화되어 표준을 개발해왔다. 최근 들어서는 SDN(Software Defined Networks)을 위한 인터페이스 등 양자 키 분배망(QKD network)과 관련된 표준 개발도 시작했다.

2.4.2 국제전기통신연합 전기통신표준화부문 (ITU-T)

ITU-T의 SG13에서 양자 키 분배망과 관련된 다양한 표준들이 제정되었거나 개발되는 중이다. 한국 주도로 개발된 세계 최초의 양자 키 분배망 구조표준(Y.3800)을 비롯하여 기능별 요구사항, 키 관리 기능, 제어 및 관리, 서비스 품질보장 요구사항, 서비스 품질 보장을 위한 기능별 구조, 역할 기반 비즈니스 모델, 멀티 벤더 연동구조, 양자 인터넷을 위한 기술보고서처럼 양자키 분배 시스템을 네트워크화하는 데 필요한 다양한 표준을 개발하는 중이다.

ITU-T의 SG17에서는 양자 키 분배망의 보안 이슈와 관련된 표준들이 제정되었거나 개발되는 중이다. 양자 키 분배망의 보안 요구사항, 신뢰노드, 제어 및 관리를 위한 보안 요구사항, 암호키 조합을 통한 비밀키 공급처럼 양자 키 분배망을 구축하는 데 꼭 고려되어야 할 보안 이슈들을 표준화하고 있다.

ITU-T의 SG11에서는 최근 양자 키 분배망을 구축하기 위한 프로토콜들을 개발하기 시작했다. SG13에서 만든 구조들을 토대로 각 계층(Layer)별 인터페이스에 구체적으로 적용될 프로토콜들을 개발하는 중이다.

이렇게 3개의 SG에서 30개가 넘는 표준들이 제정되었거나 개발되는 중이다. 본문에서 소개하는 국제 표준화 기구들 중 가장 활발히 활동이 이루어지고 있는 곳이다.

2.4.3 ISO/IEC JTC1 SC27 WG3

WG3는 양자 키 분배 시스템의 시험 및 평가 방법을 위한 표준을 개발하는 중이다. 양자 키 분배 시스템은 기존 암호시스템과는 다른 새로운 방식이라 기존 보안 인증 체계를 그대로 적용할 수 없다. 이를 위해 양자 키 분배 시스템을 위한 새로운 시험 평가 방법 표준을 개발하는 중이다.

3. 맺음말

2019년 구글이 발표한 양자컴퓨터 시커모어는 세계 최초로 양자 우월성을 달성하였다. 새로운 슈퍼 컴퓨터를 얻었다는 기대와 함께 풀지 못했던 다양한 문제들을 해결할 수 있으리라는 기대를 한몸에 받고 있다. 빅데이터, 인공지능, 머신러닝, 신약 개발, 교통/물류 문제처럼 현대

의 컴퓨터로 해결하기 힘든 문제들을 해결할 수 있을지 다양한 시도들이 이뤄지고 있다.
하지만 양자컴퓨터는 인류가 이룩한 정보 시스템의 보안 체계를 위협하기도 한다. 세계에서 가장 널리 쓰이는 RSA 암호 시스템은 이미 공격을 받았으며, 다른 알고리즘들도 조금씩 위험에 노출되고 있는 실정이다. 인공지능, 머신러닝 알고리즘의 발달로 아직 알려지지 않은 새로운 공격과 위협이 생겨날 가능성도 있다.
다행히 위협받는 보안 시스템을 대체하기 위한 다양한 방법들도 제안되고 있으며, 그 안전성은 다양하게 검증되고 있다. 아직까지 본격적인 상용화를 위해서는 해결해야 할 문제들이 많고 정책적 지원이 절실한 상황이지만, 그럼에도 불구하고 앞으로도 정보 시스템을 안전하게 지킬 수 있을 것이란 기대를 갖게 한다.
특히 양자역학적 특성을 활용한 양자 암호 기술은 자연 현상에 기반하여 그 안전성을 보장하고, 수학적 분석에도 대응할 수 있는 장점을 가지고 있다. 현대 암호기술이 생긴 이래 약 100여 년 만에 생긴 위협을 극복할 수 있는 토대가 됨은 물론 미래 보안기술의 큰 축을 담당할 수 있을 것이다.
우리나라는 아직 양자 암호 분야에서는 선진국들의 기술을 추격하는 단계지만, 훌륭한 정보통신 인프라와 열정적으로 연구하는 연구자들이 있다는 장점이 있다. 또 정부는 디지털 뉴딜의 양자암호통신 시범 인프라 사업을 추진하는 등 많은 관심을 갖고 투자를 늘려가고 있다. 정부의 공격적인 지원과 산학연의 노력이 합쳐진다면 곧 한국만의 독자 기술을 확보하고 세계적으로 기술을 선도할 수 있으리라 기대해 본다.

[참고문헌]

[1] https://seed.kisa.or.kr/kisa/intro/EgovHistory.do
[2] https://ko.wikipedia.org/wiki/%EC%8A%A4%ED%82%A4%ED%85%8C%EC%9D%BC
[3] https://ko.wikipedia.org/wiki/RSA_%EC%95%94%ED%98%B8
[4] A blueprint for building a quantum computer, https://dl.acm.org/doi/10.1145/2494568
[5] Algorithms for quantum computation: discrete logarithms and factoring, https://ieeexplore.ieee.org/abstract/document/365700
[6] A fast quantum mechanical algorithm for database search, https://dl.acm.org/doi/pdf/10.1145/237814.237866
[7] Quantum Mechanics Helps in Searching for a Needle in a Haystack, https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.79.325
[8] Quantum cryptography: Public key distribution and coin tossing https://researcher.watson.ibm.com/researcher/files/us-bennetc/BB84highest.pdf
[9] Quantum cryptography and quantum cryptanalysis https://ntnuopen.ntnu.no/ntnu-xmlui/handle/11250/249693
[10] https://csrc.nist.gov/Projects/post-quantum-cryptography

※ 출처: TTA 저널 제199호