양자 키 분배 프로토콜

유튜브 주소 : https://youtu.be/pIwUjKZS9u0

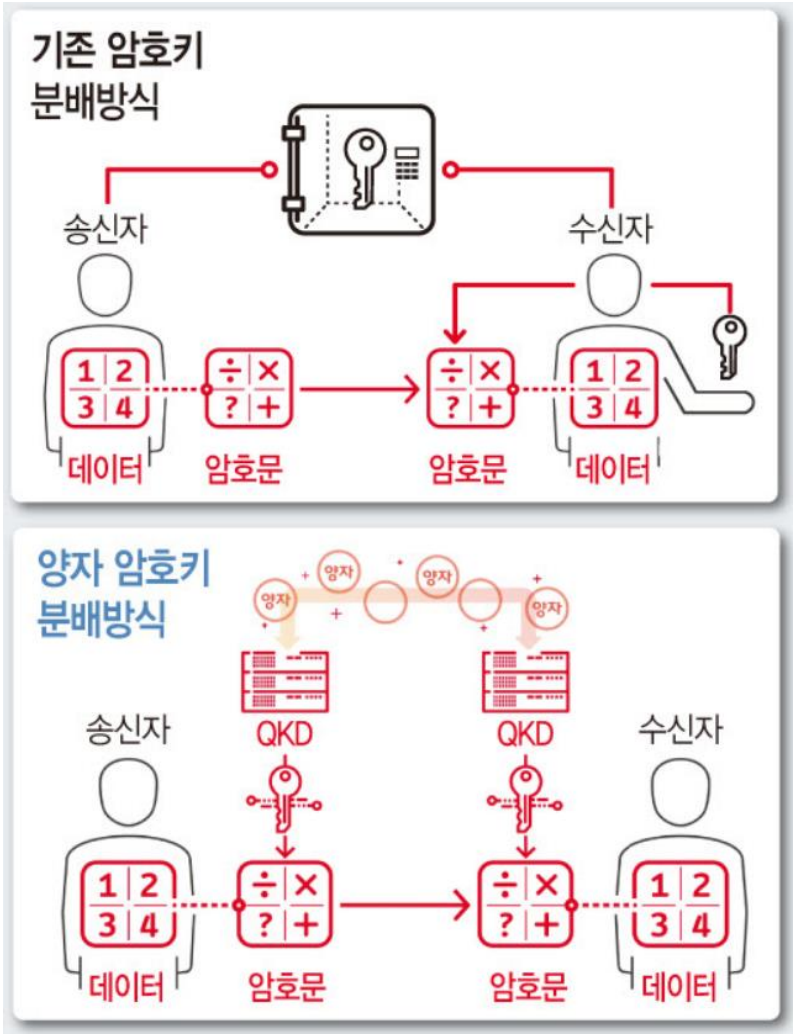
양자 통신

- 양자역학에 기반을 둔 새로운 통신방식
- 기존 암호통신보다 더 뛰어난 보안성을 제공하고자 제안
- 양자들이 가지고 있는 중첩성을 이용
  - 양자 상태 : 0 or 1의 정보의 중첩성을 지님 -> 50:50의 불확정성
- 기존의 통신 - 전자기파(빛)을 이용
  - 파장, 진폭의 차이에 의한 정보를 입력
- 양자 통신 – 빛의 편광성, 간섭현상을 이용해 정보를 구분하여 입력

양자 통신

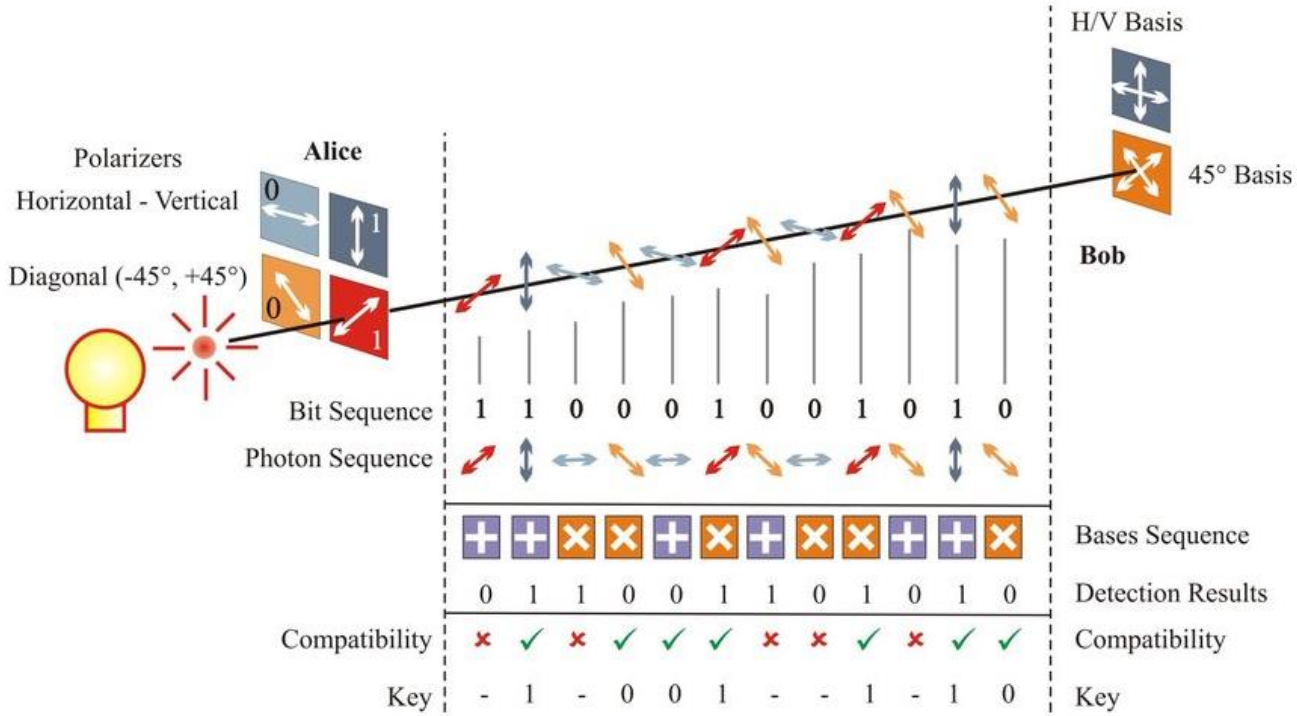
- 양자 암호 통신 네트워크 구조
  - 양자 키 분배(QKD)
  - 키 관리 시스템(KMS)
  - 암호화 장비

- 양자 키 분배(QKD) – 양자 통신 핵심 기술
  - 동일한 암호키를 생성해 송,수신자에게 전송
  - 공개 채널과 양자 채널로 연결
  - 공개 채널 – 기존의 TCP/IP 프로토콜 활용
  - QKD 프로토콜 – BB84 프로토콜 사용



BB84 프로토콜

- 1984년 IBM의 찰스 베넷, 길레스 브라사드가 제안
- 송신자와 수신자 간 비밀키 공유, OTP 생성하는 프로토콜
  - OTP(one-time password) : 일회용 인증번호
- 양자 키 분배 기술 중 이론적인 안전성이 증명된 프로토콜
- 편광과 필터를 이용
  - 광자에 편광 성질을 부여해 전송
  - 수신한 광자를 편광 필터로 측정



BB84 프로토콜 동작 과정

- 송신자(Alice)가 랜덤 한 비트 수열을 정함
- 각각의 비트를 편광시킬 편광 판을 임의로 선택
- 결정한 두 랜덤 수열을 바탕으로 각각의 랜덤 한 비트를 편광
- 수신자(Bob)에게 전송

- 편광판에 따른 비트의 편광 결과

	십자형(+)	대각형(x)
0	—	/
1	|	\

BB84 프로토콜 동작 과정

- Bob이 임의의 편광판을 사용하여 전송된 광자를 측정
- Alice가 보낸 광자 중 일부는 수신하지 못할 수도 있음
  - 양자 채널의 잡음 등의 이유로 손실 가능

- 전송된 광자 측정 결과

Bob 수신 편광 Alice 전송 신호	십자형	대각형
—	—	/ 또는 \
|	|	/ 또는 \
/	— 또는 |	/
\	— 또는 |	\

BB84 프로토콜 동작 예시

- Alice가 랜덤한 수열 두 개를 생성

비트 정보	0	1	0	0	1	1	1	0	1	0
편광판 정보	0	1	1	0	1	0	1	1	1	0

- 편광 판으로 편광한 광자를 Bob에게 전송

편광된 광자	—	\	|	—	\	|	\	/	\	—

- Bob은 Alice에게 받은 광자를 임의로 정한 편광판 순서대로 측정
  - 이 때 일부 광자를 수신하지 못함을 상정(1번째와 5번째로 전송된 광자 손실)

비트 정보	1	1	0	1	1	0	0	1	1	1
편광판 정보	x	\	I	\	x	|	—	/	\	/

BB84 프로토콜 동작 예시

- Bob은 수신한 광자에 대한 정보를 Alice에게 전송
  - 광자를 측정하는데 필요한 편광 판 정보도 함께 전송

수신한 광자위치	2	3	4	6	7	8	9	10
편광판 정보	1	0	1	0	0	1	1	1

- Alice는 Bob이 측정한 광자의 위치에 대응하는 편광 판 정보를 Bob에게 전송

편광판 정보	1	1	0	0	1	1	1	0

- Alice와 Bob은 서로 같은 편광 판을 사용한 위치의 비트를 비밀키로 공유

비밀키	1 1 0 1

Q & A