양자암호통신 Quantum Cryptography Communication

일반 VPN vs Q-VPN

일반 VPN

1. 알려진 취약점(유사난수 알고리즘)을 공략해 암호를 해독하여 공격
   -양자 컴퓨터는 해독 시간을 극단적으로 단축
2. 복호화 키를 훔치는 방법으로 공격
   -다수의 키 획득 시 유사난수생성 패턴 파악 가능

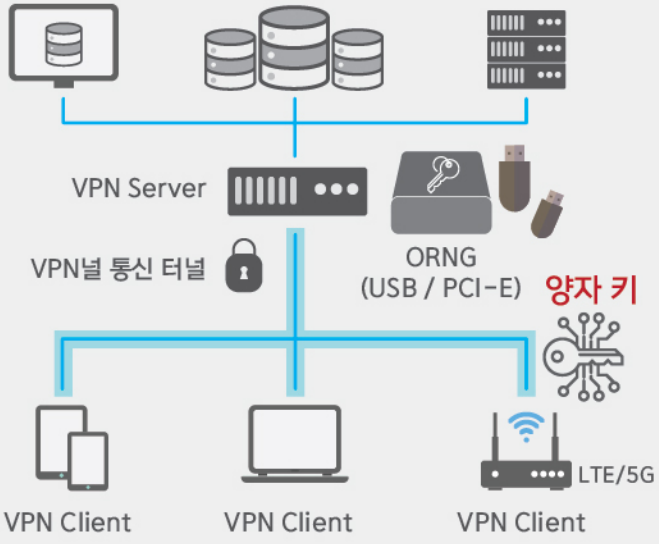
Q-VPN

1. 양자 키는 이론적/수학적으로 예측과 재생성 불가
   -알고리즘 기반 유사 난수가 아닌 순수 난수인 양자 난수 활용
2. 주기적인 양자 키 갱신으로 중간자 공격(도청) 행위 방어
   -다수의 키 획득 시 유사난수생성 패턴 파악 가능

양자 난수 특징

특성	Gaussian Pseudo Random Number	Quantum Random Number
무작위성	X	O
예측 불가능성	X	O
예측 불가능성	X	O

Q-VPN 동작 방식



01 **SSL Handshake**
양자 키 분배를 위한 컨트롤 채널 생성

02 **컨트롤 채널을 통해 인증 정보 교환**
데이터 채널에 사용할 VPN 설정 정보, 인증 정보 송수신

03 **양자 키 생성**
QRNG로 생성된 Random Number 기반으로 암호키 생성

04 **데이터 채널 생성**
양자 키 전달 후 데이터 채널 생성

05 **SSL 보안 통신**