White Paper

AhnLab TrusGuard Q-VPN
해독 불가한 암호화 기술 탑재

양자 컴퓨터의 등장은 연산 속도를 획기적으로 앞당기게 된다.
→ 기존 암호 체계를 무너뜨릴 가능성 대두

개요

2019년 9월, 구글은 자사의 양자 컴퓨터 칩 '시커모어(Sycamore)'로 양자 우월성을 세계 최초로 달성했다는 내용을 미항공우주국(NASA) 웹사이트에 게시했다가 삭제했다. 다만, 그 직후 국제 학술지 '네이처' 온라인판에 정식 논문을 공개했으며, 그 핵심 내용은 다음과 같다.

현존 최고 슈퍼 컴퓨터로도 1만 년 계산해야 풀 수 있는 수학 문제를
구글의 시커모어는 단 200초(3분 20초) 만에 해결

해당 논문을 기반으로 한 슈퍼 컴퓨터와 양자 컴퓨터의 비교와 해당 내용이 우리에게 주는 시사점은 아래 표와 같다.

구분	슈퍼 컴퓨터	양자 컴퓨터
특징	범용 연산	병렬 연산 특화 (난수, 소인수 분해, 신약 개발, AI 등)
성능 표현	플롭스 (1PF = 초당 1000조 개의 계산)	큐비트(Qubit) (53개 큐비트 = 9007조 개 동시 계산)
제품 비교	IBM 서미트(148PF) 난수 증명 = 1만년	구글 시커모어(53 Qubits) 난수 증명 = 3분 20초
로드맵	2023년까지 1000 큐비트 개발 계획	72 + α(수백 ~ 수천)
의견 차이	최적화 시 2.5일로 연산 시간 단축 가능 하지만, 양자 우월성 도달은 아님	난수 증명에서 양자 우월성 달성 현존 최고의 양자 컴퓨터 칩
시사점	양자 컴퓨터 상용화 & 범용화는 최소 10년 이상 소요 예상 상용화 이후에도 기존 슈퍼 컴퓨터 대체가 아닌 특정 용도로 사용 특정 용도에 소인수 분해 포함 → 기존 암호 체계 무너뜨릴 가능성	

AhnLab TrusGuard에
Q-VPN 탑재
KT와 공동으로 개념 검증(PoC)
진행 중

한 가지 확실한 점은 양자 컴퓨터가 특정 분야에서 기존 컴퓨터를 월등히 뛰어 넘는 성능을 보인다는 것이다. 문제는 이 특정 분야가 병렬 연산이라는 것이고 기존 암호 체계에서 사용되는 의사난수, 소인수 분해 등이 이에 해당된다. 즉, 양자 컴퓨터가 상용화 & 범용화 되면 기존 암호 체계를 모두 무너뜨릴 가능성도 있다.

이미 세계 각국에서는 양자 컴퓨팅은 물론, 양자 우월성에 대응할 수 있는 양자암호통신 기술과 양자내성암호에 대한 공격적이고 활발한 연구 및 투자를 진행 중이다.

안랩의 Q-VPN 사업 현황

안랩 또한 이러한 세계적인 보안 트렌드에 맞춰 지난 2020년 9월부터 12월까지 '양자암호통신 디지털 뉴딜 1차년도 사업'의 산업 분야에 KT, 한국과학기술연구원(KIST), 현대중공업과 컨소시엄을 구성해 참여했다. 양자암호통신과 관련된 다양한 기술 중 응용 서비스인 Q-VPN 개발을 안랩이 담당하였고 현재는 이를 현대중공업에 성공적으로 구축하여 운영 중이다.

해당 사업의 양자암호통신은 QKD(Quantum Key Distribution, 양자키분배)가 핵심 요소인데 아직까지는 높은 가격대와 전용 광통신 선로의 필요성으로 인해 본격적인 상용화는 조금 더 시일이 걸릴 것으로 예상된다.

안랩은 KT와 디지털 뉴딜 사업의 연장선으로 QKD를 제외하고 QRNG(Quantum Random Number Generator, 양자난수생성기)를 활용한 양자암호통신 기반의 Q-VPN(Quantum-VPN) 솔루션의 PoC(개념 검증)를 진행하고 있다.

QKD를 제외하더라도 중간자 공격에 대한 일정 수준 이상의 보안성을 제공할 수 있기 때문에 빠르게 상용화가 가능한 양자암호통신 기반의 VPN 솔루션을 제공할 수 있게 된다. 이를 통해 양자 컴퓨터의 본격 등장에 대비하고자 하는 국내외 다수 고객들의 보안성 강화 요구를 완벽하게 수용할 수 있다.

Q-VPN은 왜 필요한가

Q-VPN이 필요한 이유는 앞서 언급한대로 양자 컴퓨터의 뛰어난 병렬 연산 성능에 대응하기 위함이다.

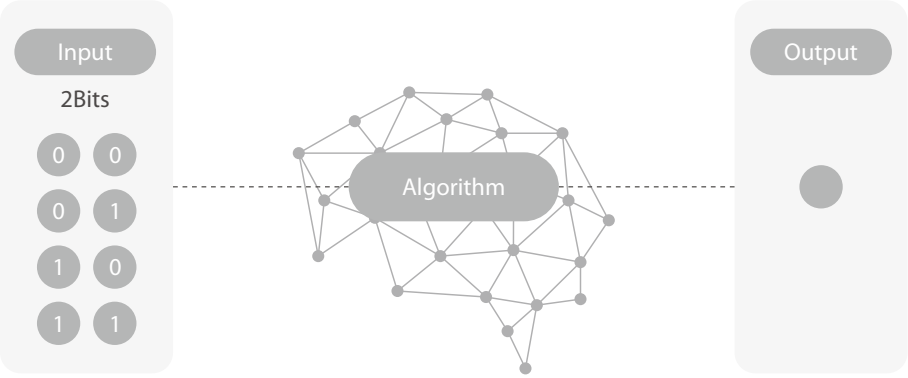
양자 컴퓨터는 기존 컴퓨터와는 전혀 다른 방식으로 큐비트(Qubit)를 사용하는데 양자역학에 따라 큐비트가 증가할수록 연산 능력은 지수적으로 증가하게 된다. 예를 들어,

안랩 Q-VPN의 가치 1

계산이 불가능한 양자암호통신 기술로 양자 우월성에 대한 해답 제시

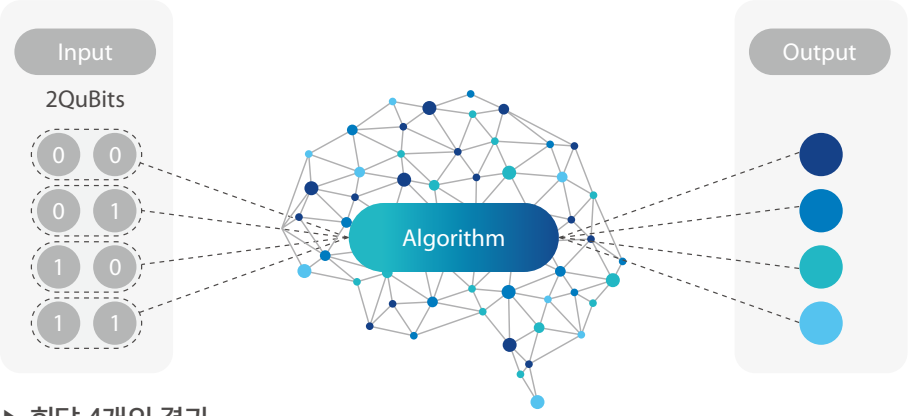
큐비트가 2개인 경우 1회에 4번의 연산을 동시 수행 가능하고 큐비트가 53개인 경우 1회에 2의 53제곱인 약 9천조번의 연산을 동시 수행 가능하다. 이는 곧 계산 가능한 암호 체계의 개선이 필요함을 뜻한다. 특히 양자 우월성에 대한 대응 방안으로 계산이 불가능한 양자암호통신 기술이 필요하며, 안랩의 Q-VPN이 이에 대한 해답이 될 것이다.

일반 컴퓨터 연산 방식 : 비트 수가 늘어나도 성능과는 무관



▶ 회당 1개의 결과

양자 컴퓨터 연산 방식 : 큐비트 수가 늘어날수록 기하급수적으로 성능 증가



▶ 회당 4개의 결과

일반 VPN vs Q-VPN

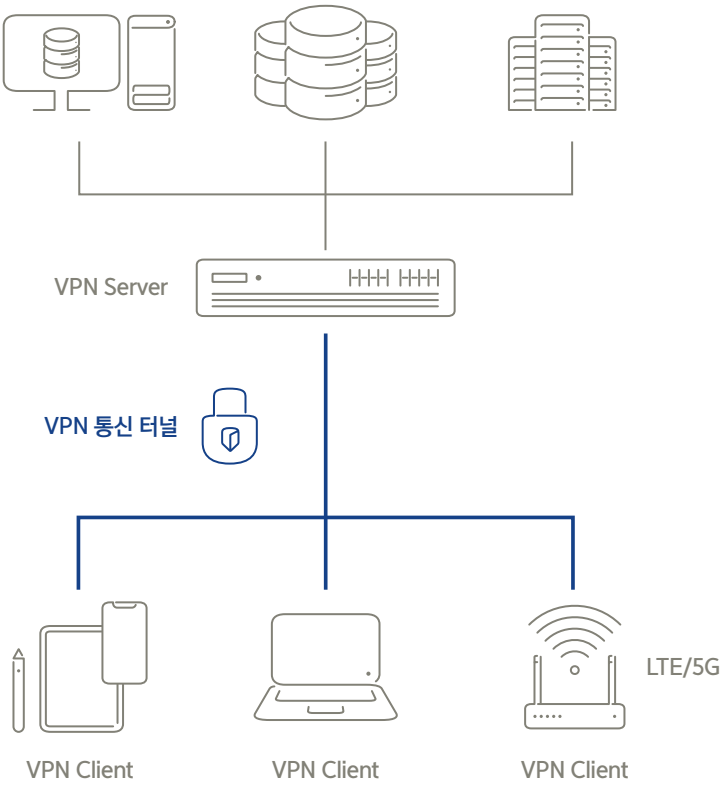
미국 국가안보국(NSA) 내부 고발자 에드워드 스노든(Edward Snowden)에 의하면 현재의 VPN을 공격하는 방법은 두 가지가 있다. 첫째, VPN은 정형화된 소수와 의사난수를 사용하는 알고리즘 기반이기 때문에 충분한 비용(1억 달러)과 충분한 시간(1년)을 들이면 해독 가능하다고 폭로했다. 양자 컴퓨터를 활용한다면 이 시간은 더 극단적으로 단축된다. 둘째, 복호화 키를 훔치는 방법으로 공격이 가능한데 주기적인 키 갱신을 통한 예방책도 결국 공격자가 다수의 키 수열 획득 시, 패턴 파악이 가능하기 때문에 보안이 취약해질 수 밖에 없다.

안랩 Q-VPN의 가치 2

서버 장비에 QRNG를 탑재해 양자난수를 활용한 암호화 통신

- 양자난수를 암호키로 사용
- 키 협상 불필요

현재의 일반 VPN 구성은 다음 그림과 같다.



순서	일반 VPN 보안 구성 내용
1	SSL Handshake
2	**키 협상 정보 및 VPN 정책 교환** 데이터 채널에 사용할 키 협상 파라미터 및 VPN 설정 정보, 인증 정보 송수신
3	**데이터 채널 생성** 키 협상 수행 및 데이터 채널 생성
4	SSL 보안 통신

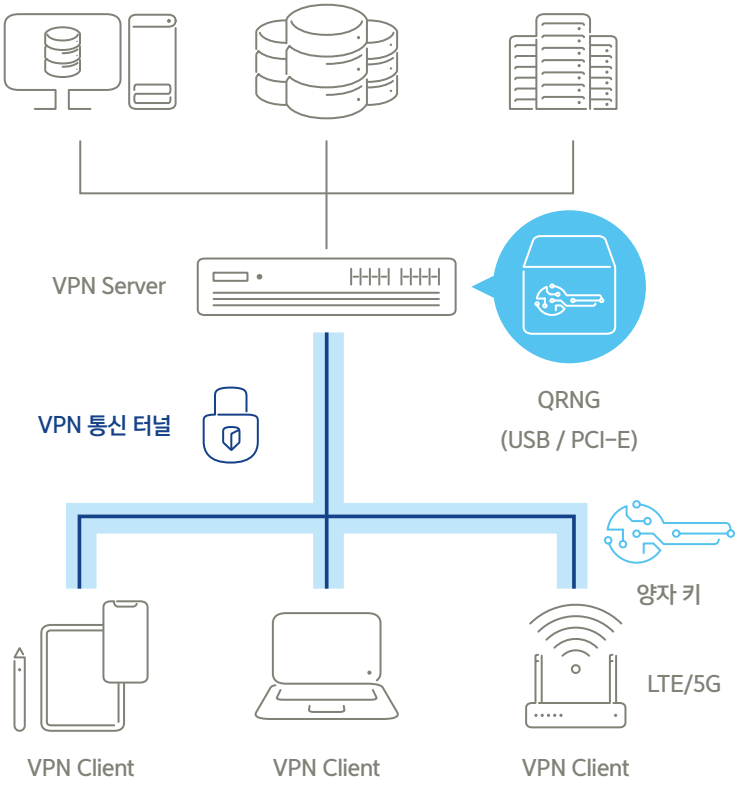
안랩의 Q-VPN은 서버 장비에 QRNG를 탑재해 의사난수가 아닌 순수난수인 양자난수를 활용하여 암호화 통신을 한다. 동작 방식에서 일반 VPN과의 차이를 정리하면 다음과 같다.

- 서버와 클라이언트 간 키 협상이 불필요해 키 협상 정보 교환도 불필요
- 양자난수를 암호키로 사용하며 서버에서 클라이언트로 키 전달을 위해 TLS 세션을 사용하여 안전한 전달 가능

안랩 Q-VPN의 가치 3

양자 컴퓨터를 사용해도 해독과 패턴 파악이 수학적으로 불가능하며, 기존 VPN 공격 방식도 무용지물

안랩 Q-VPN의 구성은 아래 그림과 같다.



순서	Q-VPN 보안 구성 내용
1	**SSL Handshake** 양자 키 분배를 위한 컨트롤 채널 생성 → 양자 키 분배를 위한 세션
2	**인증 정보 교환** 데이터 채널에 사용할 VPN 설정 정보, 인증 정보 송수신 → 키 협상 정보 교환 불필요
3	**데이터 채널 생성** 양자 키 생성 및 전달 후 데이터 채널 생성 → 키 협상 불필요
4	**SSL 보안 통신**

안랩 Q-VPN은 양자난수를 활용하기 때문에 아무리 많은 시간과 비용을 들여도, 심지어 양자 컴퓨터라 하더라도 해독이 불가능하다. 공격자가 다수의 양자키 수열 획득 시에도 패턴을 파악할 수 없다. 앞서 언급했던 일반 VPN을 대상으로 한 공격 방법은 무용지물이 되어 한층 더 높은 보안성을 제공할 수 있다.

보안을 위한 난수의 조건

난수가 해독되지 않으려면 ▲무작위성 ▲예측 불가능성 ▲재현 불가능성 등 세 가지 성질 모두를 만족하는 난수여야 한다

Q-VPN의 보안성 강화 근거

양자난수는 수학적으로 왜 양자 컴퓨터로도 해독이 불가능할까? 그 이유를 설명하기 위해 우선 난수의 성질부터 살펴보도록 한다. 난수는 아래와 같이 세 가지의 성질 중 하나 이상을 만족해야 한다.

무작위성

- 통계적인 편중 없이 수열이 무작위로 된 성질
- '아무렇게'로 보이는 성질
- 암호에 사용하는 난수는 무작위성 만으로는 불충분

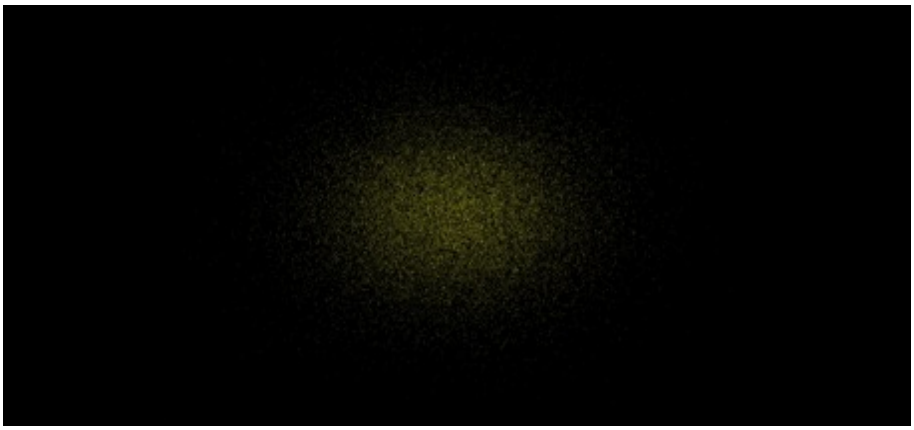
예측 불가능성

- 과거의 수열로부터 다음 수를 예측할 수 없는 성질
- 과거의 난수열이 알려져도 다음의 난수 예측 불가
- 암호 기술에 사용하기 위한 최소한의 필요 조건

재현 불가능성

- 한 난수열로부터 동일한 수열을 재현할 수 없는 성질
- 그 난수열 자체를 보전하는 것 외에 재현 불가
- 소프트웨어만으로는 재현 불가능한 난수열 생성 불가

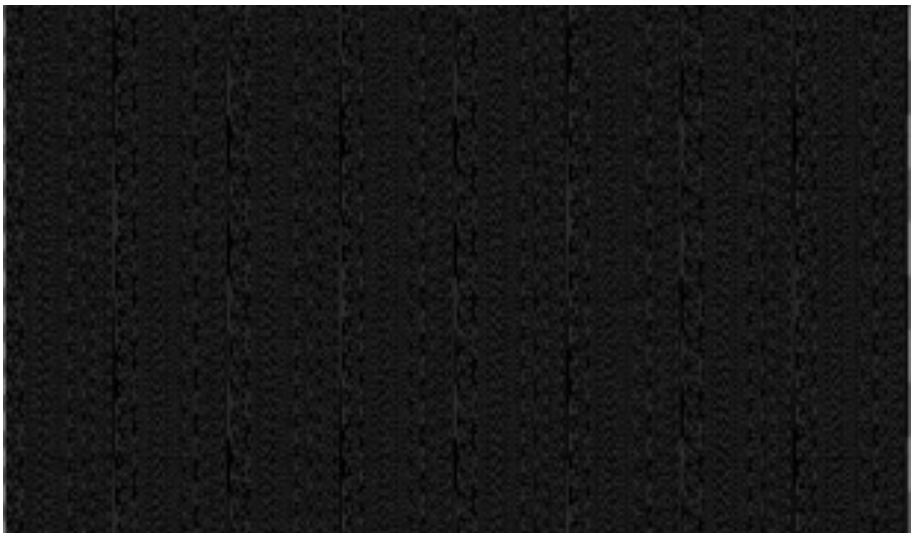
아래 그림은 의사난수 중 하나인 'Gaussian Pseduo Random Number'의 난수 분포도이다. 난수의 성질 중 예측 불가능성만 만족하며 중앙으로 편중된 분포를 보이므로 무작위성을 만족하지 못하기 때문에 암호에 사용할 수 없는 난수이다.



다음 그림은 소프트웨어 기반의 일반적인 Pseduo Random Number의 난수 분포도이다. 무작위성과 예측 불가능성은 만족하지만 일정 간격의 줄무늬 패턴을 볼 수 있다. 소프트웨어 기반이기 때문에 재현 불가능성은 만족하지 못한다.

Q-VPN이 해독 불가능한 수학적 이유

Q-VPN이 사용하는 양자난수는 난수의 세 가지 성질을 모두 충족하며, 이는 강력한 보안의 근거가 된다.



물론 알고리즘을 개선하여 분포도를 좁은 범위로 한정하면 마치 재현 불가능성을 만족하는 것처럼 나타날 수 있다. 하지만 소프트웨어 기반이므로 범위를 확장하면 결국 패턴이 나타나게 된다. 패턴의 주기가 길어지는 것일 뿐이지 반복되는 패턴 자체를 없앨 수는 없다.

암호 기술에 사용되는 난수는 무작위성과 예측 불가능성을 만족해야 하고 여기에 더해 재현 불가능성까지 난수의 세 가지 성질을 모두 만족하는 가장 강력한 난수여야 한다.

안랩 Q-VPN에서 사용하는 양자난수는 EYL의 Quantum Random Number이며 다음 그림과 같이 세 가지 성질을 모두 만족하는 가장 강력한 난수이다. 이론적, 수학적으로 예측과 재생성이 불가능하기 때문에 양자 컴퓨터로도 해독이 불가능하며, 이는 보안성 강화의 충분하고 타당한 근거가 되는 것이다.

안랩 Q-VPN 제품 구성

안랩 Q-VPN 패키지는 아래 표와 같이 서버, 클라이언트로 구성되며 임베디드 단말 연동인 경우 라우터가 추가된다.

구성 요소	내용
Q-VPN 서버	AhnLab TrusGuard 제품 + EYL의 QRNG 카드
Q-VPN 클라이언트	PC (Windows)
	모바일 (Android, iOS)
	임베디드 (LTE/ 5G 라우터)
라우터	멕서스, 머큐리의 라우터 제품

Q-VPN Server Specifications

Q-VPN 서버는 총 3가지 모델이며 상세 스펙은 다음과 같다.

구분		TG 2000BQ	TG 5000BQ	TG 10000BQ
CPU		8 Core	20 Core (10 Core *2)	32 Core (16 Core *2)
RAM		16GB	64GB	64GB
System Storage		SSD 64GB	SSD 64GB	SSD 64GB
Log Storage		HDD 2TB	HDD 2TB	HDD 2TB
Log Storage (Option)		HDD 4TB or SSD 960GB/1.92TB (RAID-1/0)	HDD 4TB or SSD 960GB/1.92TB (RAID-1/0)	HDD 4TB or SSD 960GB/1.92TB (RAID-1/0)
NIC	1GC	10 (Max 34)	10 (Max 50)	10 (Max 50)
	1GF	8 (Max 32)	8 (Max 48)	8 (Max 48)
	10GF	0 (Max 12)	4 (Max 28)	4 (Max 28)
	40GF	-	0 (Max 4)	0 (Max 8)
QRNG		USB or PCI-E	USB or PCI-E	USB or PCI-E
FW		60G	120G	200G
IPS		20G	30G	50G
VPN		10G	13G	19G
VPN Tunnel		40,000	50,000	60,000
Concurrent Session		10,000,000	30,000,000	40,000,000
Size(WxHxD)		438x88x571	438x88x571	438x88x571
Power		Redundant	Redundant	Redundant

Q-VPN 제품 구성

Q-VPN 서버 내 장착용으로 두 가지 타입의 QRNG 카드 제공

QRNG Specifications

Q-VPN 서버 내에 장착하는 QRNG 카드는 총 2가지 타입이며 상세 스펙은 아래와 같다.

USB Quantum Random Number Generator

TYPE	PARAMETER	GENERAL DESCRIPTIONS
QRNG-H	Speed	1.0 Gbps
	Operating Temperature	-20˚C to +85˚C
	Voltage	5 Volts
	Current	125 mAmps
	USB Dimensions	65mm. *23mm. *10mm.
QRNG-L	Speed	10 kbps ~ 1.0 Mbps
	Operating Temperature	-20˚C to +85˚C
	Voltage	5 Volts
	Current	60 mAmps
	USB Dimensions	44mm. *11mm. *23mm.

PCI-E Quantum Random Number Generator

PARAMETER	GENERAL DESCRIPTIONS
Speed	4 Gbps
Operating Temperature	0˚C to +60˚C
Voltage	5 Volts
Dimensions	120mm. *100mm.

앞으로의 안랩 Q-VPN

- CC 인증 획득 진행 중
- VPN 외에도 다양한 방식으로 양자난수 활용 보안 솔루션 확대 예정

Router Specifications

Q-VPN 클라이언트가 임베디드 단말인 경우 라우터의 스펙은 아래와 같다.

LTE Router_Industrial

MXR-40KD

4G LTE	Wi-Fi	CPU	Hardware Interface	Application
DL 150 / UL 50 Mbps	802.11 b/g/n 2.4GHz	Broadcom 533MHz Single-core	WAN(1)/LAN(1)/ UART(1)	NMS / Radius / VPN client

향후 로드맵

CC 인증 획득

QRNG를 활용한 Q-VPN 기능으로 국내검증필암호모듈 검증 제도인 KCMVP 획득 및 이를 기반으로 EAL4 CC 인증 획득을 진행 중이다.

QRNG 적용 보안 솔루션 확대

VPN 뿐만 아니라 다양한 방식으로 양자난수를 활용할 수 있는 보안 솔루션을 확대할 예정이다.

결론

본 백서에서는 안랩 Q-VPN의 필요성, 사업 현황 및 주요 특징을 살펴봤다. 이제, 양자 컴퓨터의 우월성으로 인해 촉발된 기존 암호 체계의 붕괴 가능성을 대비하는 것은 물론 새로운 트렌드로 자리잡은 언택트, WFA(Work From Anywhere) 등 뉴노멀에 적응해야 하는 시대가 도래했다. 여기에 안랩 Q-VPN은 강화된 보안을 확보하기 위한 방안으로 효과적인 선택지가 될 것이다.

보안 종사자를 위한 TIP

양자 컴퓨터와 양자 암호 통신의 개념, 공통점 및 차이점에 대한 명확한 이해 필요

참고: 관련 용어

구글의 양자 우월성 달성 논문 발표 이후, '양자'는 세간의 관심을 한 몸에 받고 있으며 '양자'가 포함되는 용어의 출현 빈도도 높아졌다. 그 중에서 알아두면 좋을 만한 용어를 아래와 같이 정리했다. 특히 보안 관련 종사자라면 두 번째 항목까지는 확실하게 알아 두는 것이 도움이 될 것이다.

양자 컴퓨터, 양자 암호 통신

- 구현 상의 관련성 없음
- 양자 컴퓨터 상용화 시 기존 암호 체계가 무너지는 것에 대한 대응 방안으로 양자 암호 통신 등장

양자 암호 통신 vs. 양자 내성 암호

- 공통점 : 양자 컴퓨터의 양자 우월성을 대응하기 위한 목적
- 차이점:

– 양자 암호 통신 : 자연 현상(양자역학)에 기반을 둔 기술로 이론적으로 계산 불가능

– 양자 내성 암호 : 격자 기반 알고리즘으로 이론적으로 계산 가능하지만 양자 컴퓨터로도 계산이 매우 어려움

양자 암호 통신, 양자 통신, 양자 전송

- 양자 암호 통신 : QKD 또는 QRNG를 활용한 암호 통신
- 양자 통신 : 거리에 관계없이 즉시 정보 전달(양자 얽힘)
- 양자 전송 : 양자 상태 정보 전달(ex. 시공간 이동)

양자 역학(Mechanics) vs. 양자 물리학(Physics)

- 같은 의미로 사용 되지만 양자 역학이 바람직한 표현
- 물리학은 이를 더 넓은 범위에서 지칭하는 표현

양자 역학 vs. 입자 물리학

- 양자 역학 : 분자 단위 이하의 미시계 현상 연구
- 입자 물리학 : 가장 작은 기본 입자(쿼크, 렙톤 등) 연구

AhnLab

경기도 성남시 분당구 판교역로 220 (우)13493
홈페이지: www.ahnlab.com
대표전화: 031-722-8000 팩스: 031-722-8901