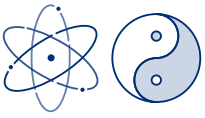
AhnLab TrusGuard

Q-VPN: 양자암호통신 기반 해독 불가한 암호화 기술

AhnLab TrusGuard Q-VPN은 Post Quantum 시대
양자 우월성에 대응할 수 있는 차세대 VPN 입니다.

배경



2019년 9월, 구글은 국제 학술지 '네이처'에 자사 양자 컴퓨터 칩 '시커모어(Sycamore)'로 양자 우월성을 세계 최초 달성했다는 내용을 정식 논문을 통해 공개했습니다. 다음은 논문의 주요 내용입니다.

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

탁월한 연산 능력을 보유한 양자 컴퓨터가 본격적으로 활용되면 현재의 암호 체계를 무너뜨릴 가능성이 있습니다. 다만, 막연한 우려에 휩싸이기 보다는 양자 컴퓨터에 대한 정확한 정보를 파악하여 대응해야 합니다. 다음은 양자 컴퓨터에 대한 설명과 '팩트체크' 사항입니다.

구분	설명	팩트체크
용도	· 특별한 공식 없이 모든 경우의 수를 탐색하는 연산	· 아직 실용 가능한 알고리즘 부족
성능 표현	· 큐비트 (Qubit) (53개 큐비트 = 9,007조 개 동시 계산)	· 오류 정정에 다수의 큐비트 사용
특징	· 큐비트 수에 따라 지수적 성능 증가	· 양자 상태 유지 난이도 증가
로드맵	· '23년까지 1,000 큐비트 개발 계획	· 100만 큐비트는 되어야 실용 가능
'19년 구글 양자 우월 달성	· 구글 시커모어 (53 Qubits) 난수 증명 = 3분 20초	· 슈퍼컴퓨터로 알고리즘 튜닝 시 2.5일
위험성	· 기존 암호 체계 무너뜨릴 가능성	· 공개키 방식 알고리즘 위험 · 대칭키 방식은 키 사이즈를 두 배로 늘리는 것으로 동일 보안 가능

양자 암호 기술	· QKD/QRNG: 계산 불가능 · PQC, 동형 암호, zk-STARKs: 계산이 어렵고 오래 걸림

양자 컴퓨터의 상용화에 대비하기 위해 근본적으로 계산이 불가능하거나 양자 컴퓨터로도 계산이 어려운 양자 암호 기술의 필요성이 대두되고 있습니다. AhnLab TrusGuard Q-VPN에 적용된 기술은 계산이 원천적으로 불가능한 '양자난수'를 기반으로 합니다.

양자암호기술

양자암호기술은 크게 두 가지가 있습니다. 첫째는 '양자' 자체를 암호에 활용하는 기술로, QKD(Quantum Key Distribution, 양자키분배기)나 QRNG(Quantum Key Distribution, 양자난수생성기)를 활용한 양자암호통신입니다. 둘째는 양자를 활용하는 것이 아닌 '양자 컴퓨터'의 뛰어난 연산 성능에 대응이 가능한 암호기술입니다. PQC(Post Quantum Cryptography, 양자내성암호), 동형암호, 영지식 증명 등이 있습니다.

* HE : Homomorphic Encryption, 동형암호
ZKP : Zero Knowledge Proof, 영지식증명
zk-STARKs : zero-knowledge Scalable Transparent ARguments of Knowledge

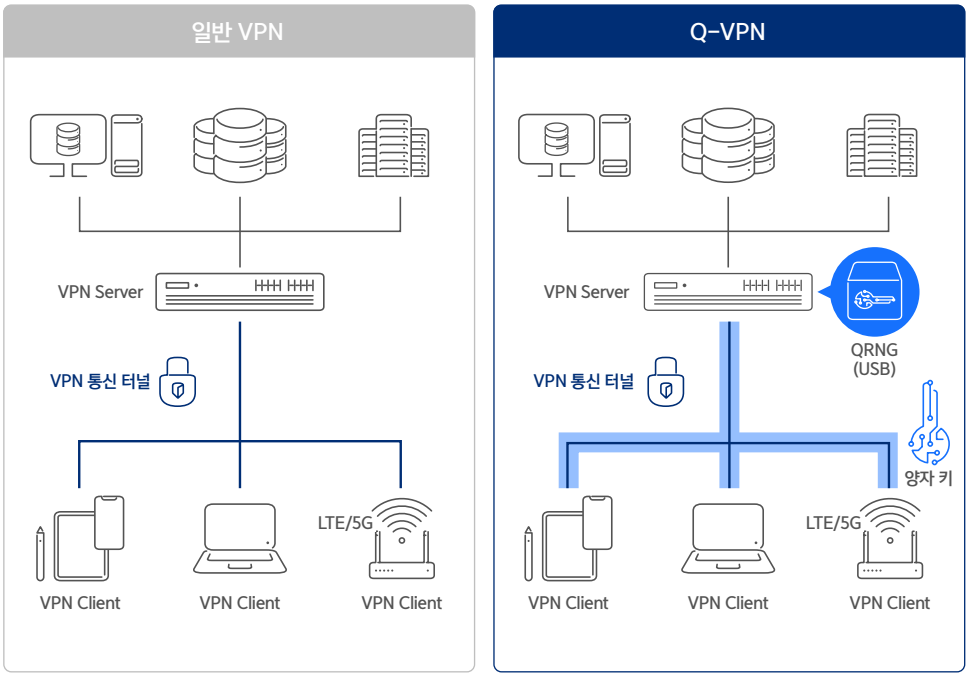
다음은 양자암호통신의 QKD와 QRNG 및 양자암호통신과 양자내성암호를 비교한 것입니다.

구분	QKD	QRNG
기능	· 양자역학적 성질을 이용한 양자키 분배 · 광자의 편광성 (BB84), 양자얽힘 (중국 묵자호)	· 양자역학적 성질을 이용한 양자 난수 생성 · 방사성 동위원소 알파 입자의 불확정성
특징	· 고가 대형 장비 (QRNG 포함) · 구축 시 광채널 (거리 제약), 암호화 장비, KMS 필요	· 초소형 칩 (Chip) 형태 · Board, USB, PCI-E 등으로 인터페이싱
보안성	· 중간자 공격 원천 방지	· 완벽한 무작위성의 난수로 패턴 예측, 재생성 불가능
제품/기능 예시	· SKT, KT의 양자암호통신망 · KREONET (국가과학기술연구망)	· 갤럭시 퀀텀, Q-VPN, Q-OTP, QLock 등
향후 로드맵	· 양자통신, 양자인터넷으로의 진화 첫 단계	· 난수를 활용한 모든 영역으로의 적용

구분	양자암호통신 (QKD/QRNG)	양자내성암호 (PQC)
원리	· 양자역학적 성질을 보이는 '양자' 자체를 활용 (H/W)	· PKI 알고리즘 (S/W) *대칭키 방식은 키 사이즈를 두 배 늘리는 것으로 동일 수준 보안 가능
특징	· 별도의 장비, 통신 설비 등 추가 도입 필요	· 기존 인프라에 바로 적용 가능, 표준 알고리즘 부재로 성능 검증 필요
보안성	· 완벽한 무작위성 난수로 중간자 공격 원천 방지 (계산 불가)	· 양자 컴퓨터로도 계산이 매우 오래 걸림
한계점	· 높은 도입 비용, 기존 인프라와의 호환성 문제	· 계산 가능한 양자 컴퓨팅 알고리즘 등장 시 취약
향후 로드맵	· 두 기술은 배타적이 아닌 상호 보완적 관계로 계속 발전해 나갈 것	

AhnLab TrusGuard Q-VPN

AhnLab TrusGuard Q-VPN은 양자암호기술 중 QRNG를 활용한 VPN입니다. 참고로 QKD를 이용한 VPN은 양자암호통신 디지털뉴딜 1차년도 사업에서 구현하여 운영 중에 있으며, 양자내성암호는 국내 또는 국제 표준 알고리즘이 등장하면 반영할 계획입니다. 아래는 기존의 일반 VPN과 QRNG를 활용한 AhnLab TrusGuard Q-VPN을 비교한 내용입니다.



1 알려진 취약점(디피헬만 알고리즘)을 공략해 암호를 해독하여 공격

- 정형화된 소수와 유사 난수
- 1024bit 소수는 충분한 비용(1억달러)과 충분한 시간(1년)으로 해독 가능
- 양자 컴퓨터는 이 시간을 더 극단적으로 단축. (ex. 구글 시커모어)

2 복호화 키를 훔치는 방법으로 공격

- 키 갱신을 통한 예방책도 결국 다수의 키 획득 시 패턴 파악 가능

1 양자키는 이론적/수학적으로 예측 및 재생성 불가

- 알고리즘 기반 유사 난수가 아닌 순수 난수인 양자 난수 활용
- 아무리 많은 시간과 비용을 투자해도, 양자 컴퓨터로도 해독 불가

2 주기적인 양자 키 갱신을 통해 복호화 키를 훔치는 행위도 무력화

- 다수 양자 키 획득 시에도 패턴 파악이 불가능

2020년	2021년
국내 VPN 업체 최초 양자암호통신 레퍼런스 확보	미래양자융합포럼의 유일한 국내 VPN 업체
2021년	**2021년**
QRNG 잡음원 KCMVP 국내 최초 획득	양자암호통신기반 VPN 국내 CC 인증 최초 획득

Q-VPN의 보안성

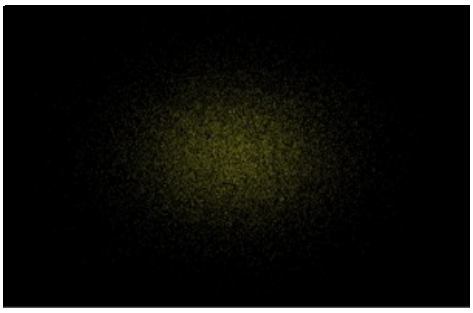
QRNG 기반 Q-VPN의 보안성은 양자난수의 품질과 직결됩니다. AhnLab TrusGuard Q-VPN에서 사용하는 EYL(이와이엘)의 QRNG는 암호화에 필요한 난수의 세 가지 성질인 ▲무작위성 ▲예측 불가능성 ▲재현 불가능성을 모두 만족하고 NIST(미국 국립표준기술연구소)의 난수 품질 평가를 충족하여 Q-VPN 양자 키의 높은 품질을 검증 받았습니다.

“ 난수의 세가지 성질 ”

의사 난수 vs. 양자 난수 보안성 비교

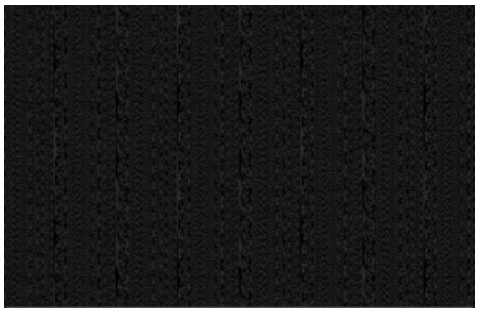
의사 난수의 한계 #1 예측 불가능성 충족

Gaussian Pseudo Random Number



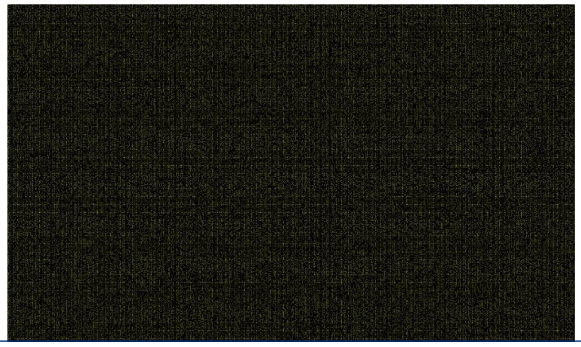
의사 난수의 한계 #2 무작위성, 예측 불가능성 충족

M사 Pseudo Random Number



양자 난수의 보안성 강화 무작위성, 예측 불가능성, 재현 불가능성 모두 충족

EYL Quantum Random Number



AhnLab TrusGuard Q-VPN의 NIST 난수 품질 평가 결과

Entropy Test	· NIST SP800-90B – Min Entropy Value : 7.87 / 8Bit · BSI AIS-31(T6~T8) – Min Entropy Value : 8 / 8Bit
Randomness Test	· NIST SP800-22 – All Condition Test : PASS · BSI AIS-31(T0~T5) – All Condition Test : PASS

주요 기능

클라이언트
PC : Windows, 한컴구름OS, 티맥스구름OS, Linux, MacOS
Mobile : Android, iOS, Wear OS (예정)
Embedded (LTE/5G Router) : MEXUS, NC&C, 아프로텍, 우진네트웍스, 우리넷 등
다양한 인증 방식
외부 인증 RADIUS, LDAP, AD, RSA SecureID (OTP), 미래테크놀로지 (OTP)
MFA (Multi Factor Authentication) : ID/PW, 사설인증서, NPKI, GPKI, FIDO, Q-SMS, Oracle DB, 자체 제공 Q-OTP
모바일 공무원증, QR Code, EPKI, ARS (예정), QLock (예정)
단말 보안
AhnLab ESA (EPP Security Assessment) 연동 - 단말 보안 상태 (보안 점수, 필수 S/W 설치 유무 등)에 따라 VPN 접속 제어
AOS (AhnLab Online Security) 연동 - 안전한 PC에서의 사용을 강제하는 기능으로써 클라이언트의 AOS 사용 강제 적용 가능
특장점
IPS 기능 지원
SSL VPN + IPSec VPN 하이브리드 구성 지원 - SSL VPN 터널을 통해 들어온 트래픽을 다시 IPSec VPN 구성망과 통신 지원 가능
ZTNA 적용 - “제어 및 데이터의 논리적 채널 분리를 통한 원격 접속 공격 표면 최소화 방안” 특허 출원 진행 중 - “물리적 망분리 환경에서 업무망 GW 주소 은닉을 통한 공격 표면 최소화 방안” 특허 출원 진행 중
NGFW 기능 지원 (예정) - 애플리케이션 기반 Micro Segmentation
부가 기능
고정 또는 동적으로 유연한 IP 할당 방식 지원
인사 DB Import : LDAP, AD, DBMS, 파일 기반 등
웹 기반 클라이언트 (예정)

Q-VPN Server Specifications

Q-VPN 서버 모델은 총 4가지이며 상세 스펙은 아래와 같습니다.

구분		TG 2000BQ	TG 5000BQ	TG 10000BQ	TG 20000BQ
CPU		8 Core	20 Core (10Core *2)	32 Core (16Core *2)	48 Core (24Core *2)
RAM		16GB	64GB	64GB	256GB
System Storage		SSD 64GB	SSD 64GB	SSD 64GB	SSD 64GB
Log Storage		HDD 2TB	HDD 2TB	HDD 2TB	HDD 2TB
Log Storage (Option)		HDD 4TB or SSD 1TB/2TB (RAID-1/0)	HDD 4TB or SSD 1TB/2TB (RAID-1/0)	HDD 4TB or SSD 1TB/2TB (RAID-1/0)	HDD 4TB or SSD 1TB/2TB (RAID-1/0)
NIC	1GC	10 (Max 34)	10 (Max 50)	10 (Max 50)	10 (Max 50)
	1GF	8 (Max 32)	8 (Max 48)	8 (Max 48)	8 (Max 48)
	10GF	0 (Max 12)	4 (Max 28)	4 (Max 28)	4 (Max 28)
	40GF	-	0 (Max 8)	0 (Max 12)	0 (Max 12)
	100GF	-	-	0 (Max 2)	0 (Max 4)
QRNG		USB	USB	USB	USB
Q-VPN Users		3,000	10,000	10,000	10,000
Size(WxHxD)		438x88x571	438x88x571	438x88x571	438x88x571
Power		Redundant	Redundant	Redundant	Redundant

QRNG Specification

Q-VPN 서버 내에 장착하는 QRNG 상세 스펙은 아래와 같습니다.

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.

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

AhnLab