JIN INFRA
ICT SMART CONVERGENCE

양자보안기술 및 진인프라 양자사업 방향

JIN INFRA
ICT SMART CONVERGENCE

CONTENTS

JIN INFRA
ICT SMART CONVERGENCE

CONTENTS

Ⅰ. 암호기술

1. 암호기술 개요

- 암호화 알고리즘

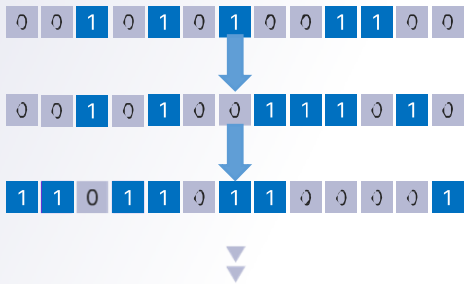
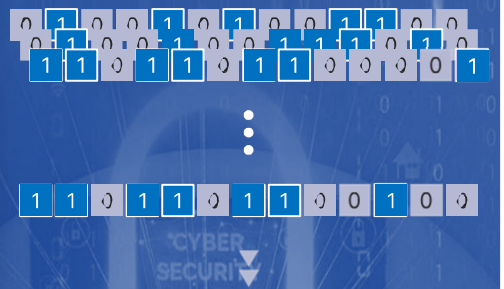
암호기술은 중요한 정보를 읽기 어려운 값으로 변환하여 제 3자가 볼 수 없도록 하는 기술

암호기술의 안전성은 수학적인 원리에 기반하며, 보안에 있어서 중요한 정보를 직접적으로 보호하는 원천기술

양방향	대칭키	Stream 방식	동기식	OTP, FSR, LFSR, NLFSR, OFB, RC4	난수열(키스트림) 독립성 생성
			비동기식(자기동기식)	CFB	난수열 종속적 생성
		Block 방식	Feistel	DES, SEED	암호화 = 복호화
			SPN	Rijndael, ARIA	암호화 ≠ 복호화
	비대칭키	RSA, ECC, ElGamal, DH			기밀성, 인증, 부인방지
일방향	해시함수	MDC	해시함수	MD5, SHA-1, RIPEMD, HAS-160	무결성
		MAC	해시함수+대칭키	축소 MAC, HMAC, CBC-MAC	무결성+인증
		전자서명	해시함수+비대칭키	RSA 전자서명, DSS, ECDSA, KCDSA	무결성+인증+부인방지

2. 양자 컴퓨터와 보안 위협

- 양자컴퓨터 개발로 RSA 암호 등을 수초 내에 암호 해독 가능

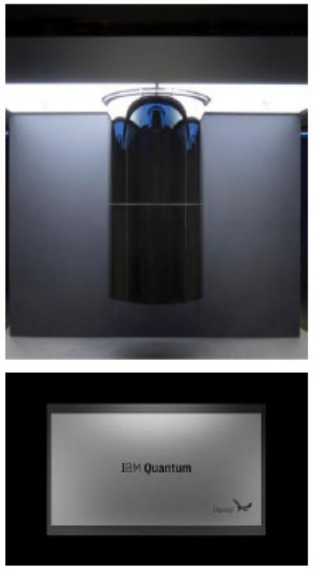
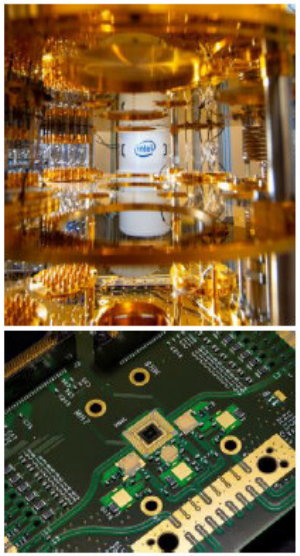
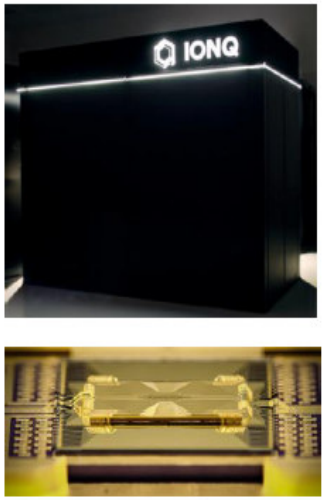
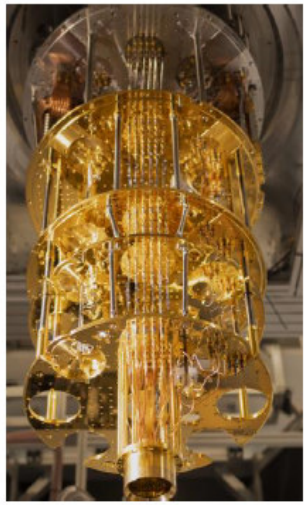
	현재컴퓨터	양자컴퓨터
	0 1 정보를 0이나 1로 표현	0 1 0과 1을 중첩
연산 개념도	 많은 시간 소요 **1개씩 순차적으로 계산**	 순식간에 합쳐서 한번에 계산
기본단위	**비트 (Bit)** 2비트면 00,01,10,11 중 한가지 정보만 처리	**큐비트 (Qubit)** 2큐비트면 00,01,10,11이 동시 존재
암호해독 소요시간	**백만 년** (계산 능력 한계)	**1초 ~ 하루 (양자병렬 계산)**

현대 암호 알고리즘의 보안 위협

알고리즘	종류	목적	양자 컴퓨터 대비사항
AES	대칭키	Encryption	키 길이 증가 필요 (Larger key sizes Needed)
RSA	공개키	Signatures, Key establishment	더 이상 안전하지 않음 (No longer secure)
SHA-2, SHA-3	-	Hash functions	출력 길이 증가 필요 (Lager output secure)
ECDSA, ECDH (Elliptic Curve Cryptography)	공개키	Signatures, Key exchange	더 이상 안전하지 않음 (No longer secure)
DSA (Finite Field Cryptography)	공개키	Signatures, Key exchange	더 이상 안전하지 않음 (No longer secure)

* NIST : 미국 국립표준기술연구소 (National Institute of Standards and Technology)

3. 양자 컴퓨터 동향

구분	IBM	Google	Intel	IonQ	Microsoft	AWS
외형						rigetti OQC IONQ IQuEra COMPUTING INC.
큐비트	433	53	12	32	-	-
방식	초전도	초전도	실리콘 스핀	이온트랩	위상 큐비트	-
서비스 (SDK)	Qiskit	-	Intel Quantum SDK 1.0	-	Azura quantum	Amazon Braket
개발년도	2022	2019	2023	2020	-	-

JIN INFRA
ICT SMART CONVERGENCE

CONTENTS

Ⅱ. 양자 보안 기술

Ⅱ 양자 보안 기술

1. 양자 보안 기술 분류

- 양자 컴퓨터 공격 대응 기술 / 양자 키 분배 & 양자 내성 암호

QKD

- 양자 키 분배(Quantum Key Distribution, QKD)

- 양자역학 특성을 이용하여 개체 사이의 키 분배하는 방법
- 이론적으로 안정성이 증명(무조건적인 절대 보안)
- 공격자의 컴퓨팅 파워가 크더라도 암호키가 노출되지 않음
- 구현형태 : 물리적 시스템으로 구성

PQC

- 양자 내성 암호(Post Quantum Cryptography)

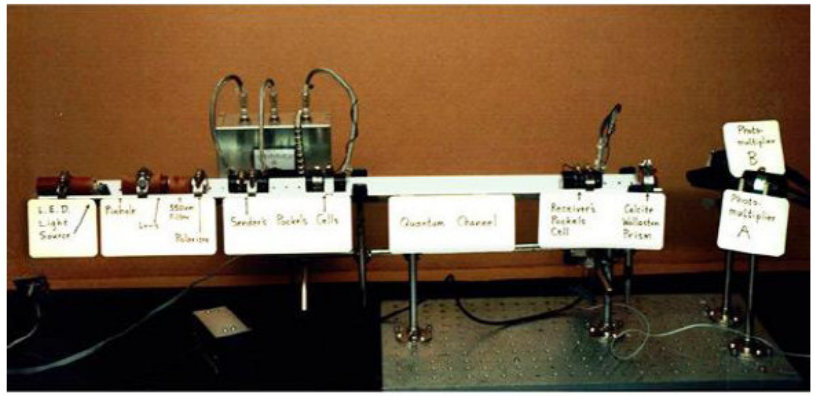
- 양자컴퓨터로도 풀기 어려운 수학적 난제(Mathematical Hard problem) 기반 설계로 보안성 확보
- 예> 격자(Lattice), 부호(Code), 해시(Hash), 다변수 방정식(Multivariate), 초특이 타원곡선(Isogeny) 등
- 현재 알려진 양자알고리즘 (Shor algorithm)과 기존 컴퓨팅 공격에 안전하다고 알려짐
- 구현형태 : 소프트웨어 하드웨어구성

2. 양자 키 분배(QKD)

-BB84 프로토콜

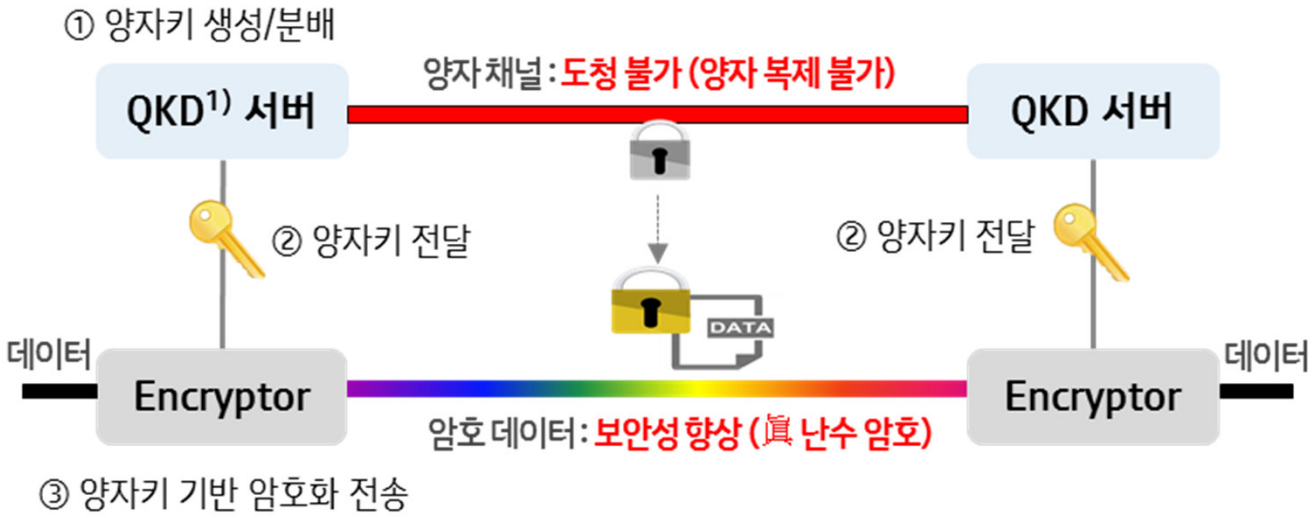
- **양자 키 분배 시스템**
  - 양자 역학의 특성을 이용한 암호키 분배 프로토콜로 구현된 보안 통신 기법
  - “Quantum cryptography: Public key distribution and coin tossing.”
    - C. H. Bennett and G. Brassard. In Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, 1984.

QUANTUM TRANSMISSION															
Alice's random bits	0	1	1	0	1	1	0	0	1	0	1	1	0	0	1
Random sending bases	D	R	D	R	R	R	R	R	D	D	R	D	D	D	R
Photons Alice sends	↗	↕	↘	↔	↕	↕	↔	↔	↘	↗	↕	↘	↗	↗	↕
Random receiving bases	R	D	D	R	R	D	D	R	D	R	D	D	D	D	R
Bits as received by Bob	1		1		1	0	0	0		1	1	1		0	1
PUBLIC DISCUSSION															
Bob reports bases of received bits	R		D		R	D	D	R		R	D	D		D	R
Alice says which bases were correct			OK		OK			OK				OK		OK	OK
Presumably shared information (if no eavesdrop)			1		1			0				1		0	1
Bob reveals some key bits at random					1									0	
Alice confirms them					OK									OK	
OUTCOME															
Remaining shared secret bits			1					0				1			1



2. 양자 키 분배(QKD)

- QKD : 암호키를 양자의 특성을 이용하여 생성/ 분배하여 암호화를 수행하는 통신



QKD 양자 암호통신 = 양자 키 분배 + 암호통신

- 양자역학의 원리를 이용하여 물리적으로 도청 불가능한 암호키 분배
- 진난수 기반 암호키 사용(Quantum Random Number Generator)
- 지속적/실시간 암호키 분배를 통해 안전성 향상

2. 양자 키 분배(QKD)

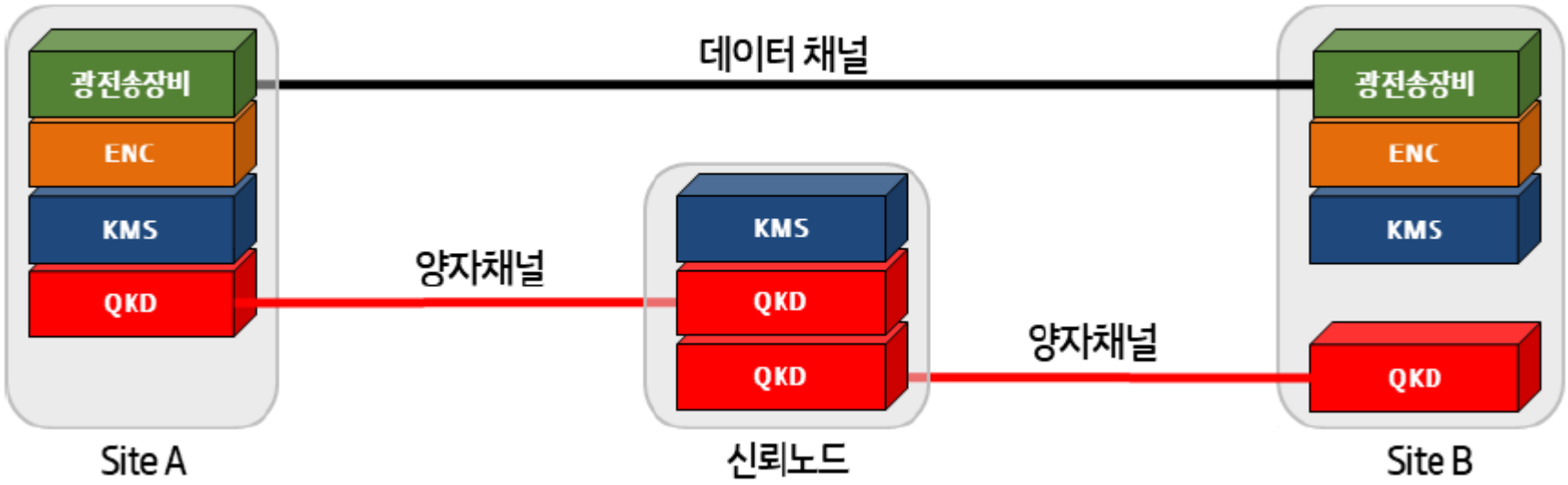
- 양자 키 분배 장치는 전송 거리에 한계 있음 이를 극복하기 위해 신뢰노드를 구성

QKD, 전송 거리에 따른 광 손실로 전송 거리 한계

- 일반적인 광 회선의 경우 0.2dB/km의 광 손실율을 가지고 있음
- QKD 시스템은 일반적으로 약 18dB (90km~120km 내외) 정도의 광 손실까지 전송 가능
- QKD 시스템은 일반적인 증폭기나 중계기의 사용이 불가능

장거리 전송을 위한 신뢰노드 구성

- QKD의 전송 거리 한계 이상으로 암호키를 전달하기 위해 신뢰노드(Trusted)를 구성하여 암호키 전달



3. 양자 내성암호(PQC)

*** 양자 컴퓨터 알고리즘**

알고리즘	특징
Shor 알고리즘	- 양자 푸리에 변환을 이용한 인수분해 푸는 시간 단축 - 비대칭키 알고리즘 복호화 단축 가능
Grover 알고리즘	- 정렬되지 않는 데이터베이스의 원소를 찾는 방식 - 대칭키 알고리즘의 복호화 단축 가능

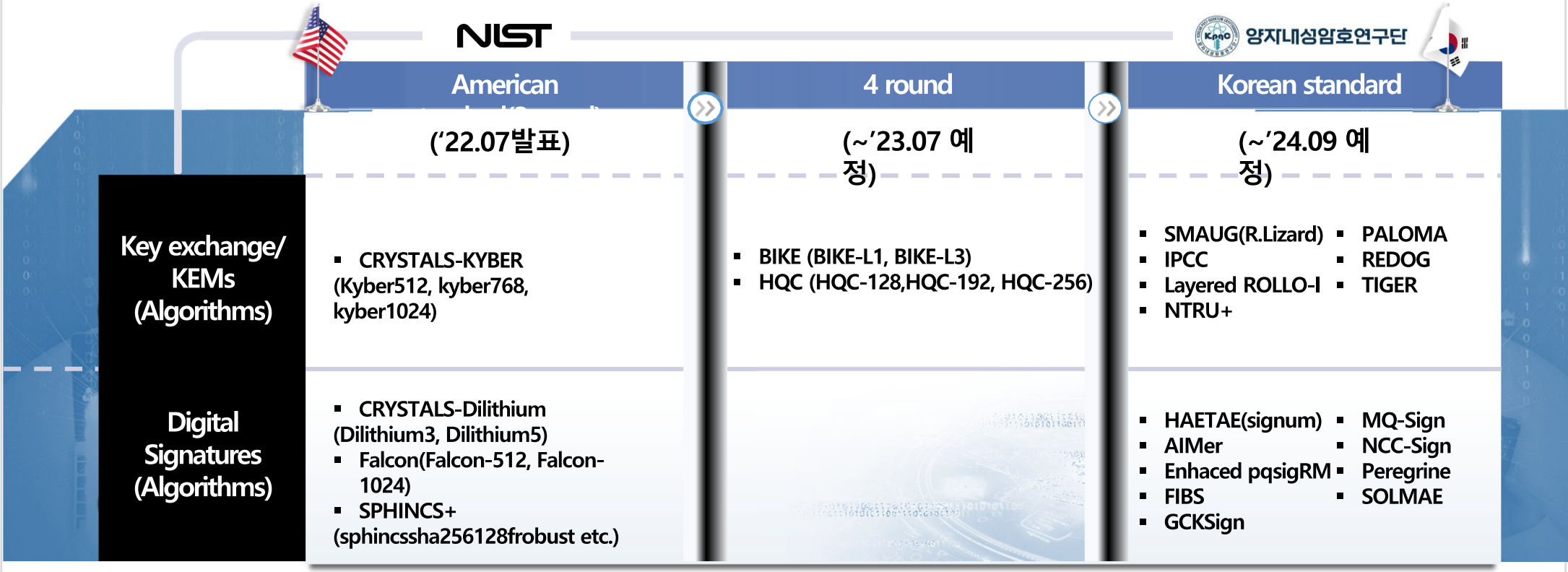
- 이에 따른, 양자 내성 암호(Post Quantum Cryptography, PQC)가 필요

-- 양자 내성 암호 구분 : 다변수 기반(Multivariate-based), 코드 기반(Code-based), 격자 기반(Lattice-based), 아이소제니 기반(Isogeny-base), 해시 기반(Hash-based) 전자 서명 등

3. 양자 내성암호(PQC)

미국 '22년 7월 1차 표준 알고리즘 4종 발표 → **'24년까지 추가 알고리즘 선정으로 미국 표준 알고리즘 확정 예정**

한국 '22년 국정원 주관으로 Kpqc 연구단 조직 → **'24년까지 한국 국가표준 PQC 알고리즘 선정 예정**



3. 양자 내성암호(PQC)

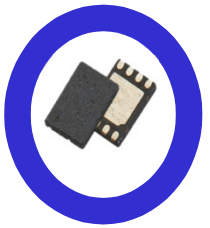
- PQC 제품군

ROADM 전송장비

PQC VPN

PQC LTE 라우터

PQC PUF USIM



PQC PUF eSIM

적용가능

컴퓨터 | 서버 | 하드웨어 | USB | 모바일 | 결제 | 개인정보 | 통합인증 | 어플리케이션

Quantum Safe Migration

JIN INFRA
ICT SMART CONVERGENCE

CONTENTS

Ⅲ. 해외 협력 업체 진행 현황

Ⅲ 해외 협력 업체 진행 현황

1. 양자보안사업 해외 협력업체 구분

업체명	American Binary	QuantLR	QuSecure	Quantum Xchange
CI				
방식	PQC	QKD	PQC	PQC/QKD(IDQ)
국가/설립일	미국/2019	이스라엘/2015	미국/2019	미국/2018, 영업(스위스)
알고리즘/프로토콜	BFF 포로토콜 Kyber 1024 VPN	BB84 Decoy state	Saber,Kyber BIKE,HQC	NIST 후보 알고리즘 지원
성능 및 기능	SDN, Firewall, VPN, SIEM Desktop Virtualization,	LoQomo1 : 100km LoQomo2 : 40~60km LoQomo3 : 5km	웹서버와 웹애플리케이션 간 양자암호 통신	PHIO TX : PQC,QRNG통합기능 PHIO TXD :양자 VPN PHIO TXC : 클라우드 활용
상품	Crypto-Agility(PQC) Fortress(SDN)	LoQomo1(QKD) LoQomo2(QKD) LoQomo3(QKD)	QuProtect TM	PHIO TX(PQC) PHIO TXD(VPN) PHIO TXC(Cloud)
비고	협력관계 체결	협력관계 체결	협력관계 체결	협력관계 체결

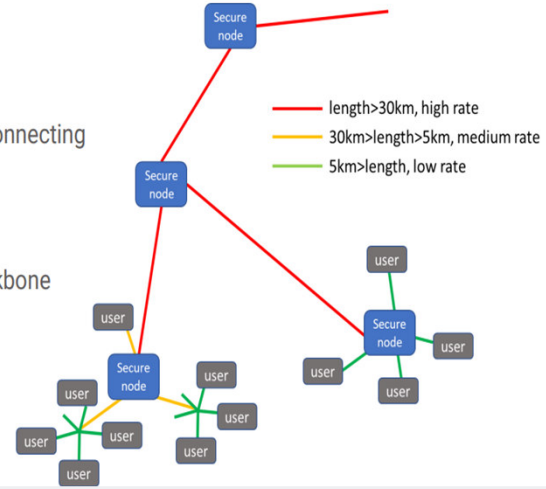
2. QunatLR

제품 선정 배경

QuantLR's unique selling proposition:

Plug-and-play solution, optimized for all network segments

- Long range, high key rate:
  - Point to point
  - Most expensive, least links, connecting local networks
- Medium range, medium key rate:
  - Point to multipoint
  - Medium cost, urban area backbone
- Short range, low key rate:
  - PON compatible
  - Low cost, "last mile", QTTx



- 현재 시장에 출시된 타(IDQ, Toshiba, 국산 등) QKD 장비 대비 가격 경쟁력 월등
- 단거리/중거리/원거리 용도 및 1:1, 1:N 토플리지 기능 제공 등 제품 종류 다양
- 계속적인 기술지원이 확실하고 국내장비 기술경쟁력 강화의 계기 마련 가능
- 하나의 1U 장비에 Alice 와 Bob을 동시 제공해 케이블 , 공간 감소, 보안성 제공

추진 내역

Comparison with IDQ offering

	Long Range		Medium range		Short Range	
	QLR LoQomo1	IDQ Clavis XG	QLR LoQomo2	IDQ Cerberis XG	QLR LoQomo3(***)	IDQ
Distance in km.(*)	100	120	40-60(**)	60	5	X
Protocol	BB84 Decoy state	BB84 Decoy state	BB84 Decoy state	COW	BB84 Decoy state	X
Security	Quantum Safe	Quantum Safe	Quantum Safe	Quantum Safe	Quantum Safe	X
Cost	$$$	$$$$$	$$	$$$	$	X

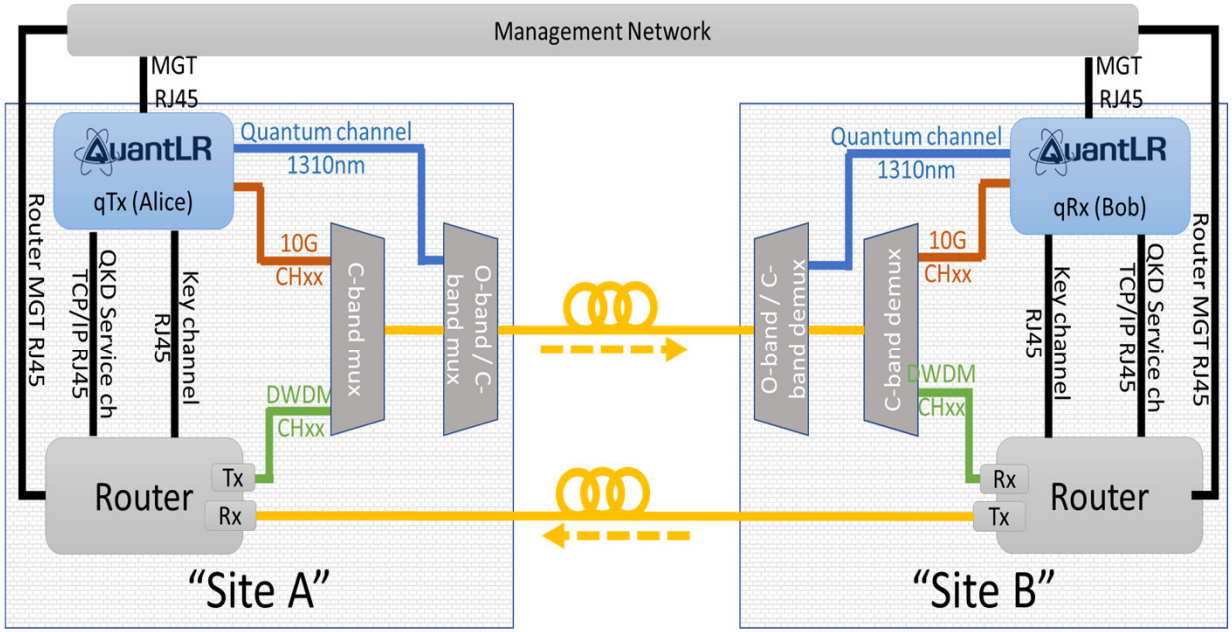
(*) 1 ksbps, dark fiber
(**) P2MP- depend on the amount of users
(***) by 2025

- 이스라엘 본사와 수차례 화상회의를 통해 장비 기술검증과 상호 신뢰도 형성
- 국내 도입을 위해 국가정보원 보안적합성 통과를 위한 사전 항목 검토
- 시에나 본사와 QuantLR과 Web 기반 Simulator를 통해 Integration 완료
- 현재 시에나 캐나다 오타와에서 QKD 장비와 전송장비 PoC 테스트 진행 중

2. QunatLR

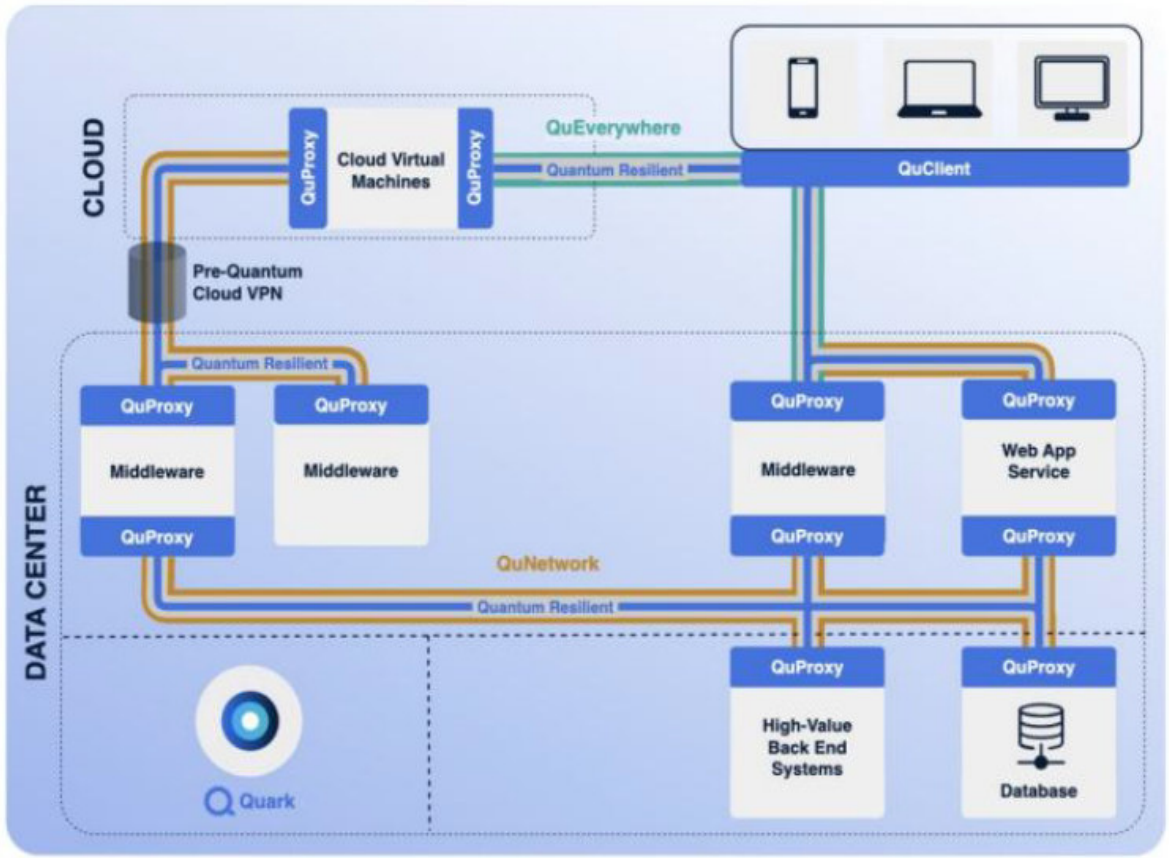
- QuantLR PoC 전체 설정

Multiplexed SMF
Quantum Channel – 1310nm SMF
Clock – DWDM channel SMF
QKD encrypted Client Data and QKD service data - DWDM channel, SMF



3. QuSecure

- 제품소개



기술 개요

- (Quark Orchestrator)에 내장된 양자기술을 사용해 모든 대상의 암호화 및 복호화, 세션 관리
- QuProtect 가 배포된 모든 네트워크에 걸쳐 보안 계층을 추가해 표준 TLS(전송계층 보안) 프로토콜 위에 PQC를 코팅
- QUEVERYWHERE
  - 코드 변경이나 클라이언트 설치 없이 PQC 적용 가능
  - 웹 서버와 웹 애플리케이션 간의 통신을 쉽게 보호
- QUNETWORK
  - 코드 변경 없이 적용 가능한 QSL 솔루션
  - 레이어4 또는 레이어7의 서비스 간 통신을 PQC 적용

3. QuSecure

- 인증 및 PoC 진행 내역

검증된 PQC 업체와의 협력 및 교류

TECHSLAYERS
기능 검증 인증

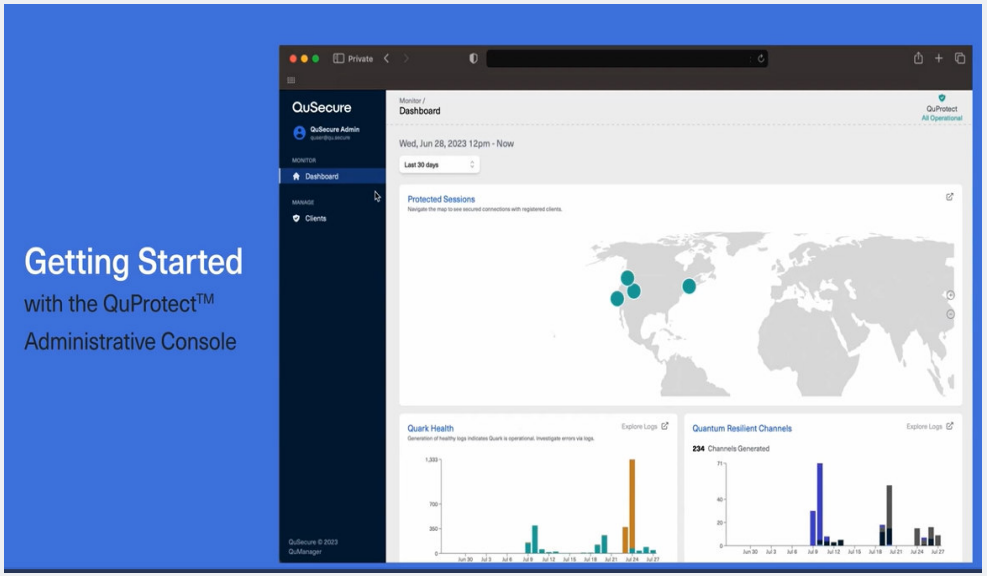
ACCENTURE
우수 기업 선정

Quantum Cybersecurity
Platinum 수상

미연방 정부 우수조달
제품으로 선정

QuSecre COO Skip Sanzeri
내한 사업 미팅

PoC 진행 내역



- QuProtect 소프트웨어 비디오 가이드를 통한 기술 검토
- Client PoC 테스트 완료
- 파트너쉽 체결 진행 중
- 파트너쉽 체결 완료 후 Quark Orchestrator 관리자 모드 PoC 진행 예정

4. Quantum Xchange

- 제품 소개

PHIO TX

- 모든 NIST 후보 알고리즘 지원
- QKD, QRNG, PQC 등 모든 방법으로 보호되는 키를 지원
- 모든 네트워크 미디어 타입에서 작동(무선, 위성,구리,광)
- 기존 네트워크 보안 제품과 쉽게 통합하여 즉시 양자암호화 가능
- 소프트웨어 방식 하드웨어 필요
- 거리제한이 없음

PHIO TXD

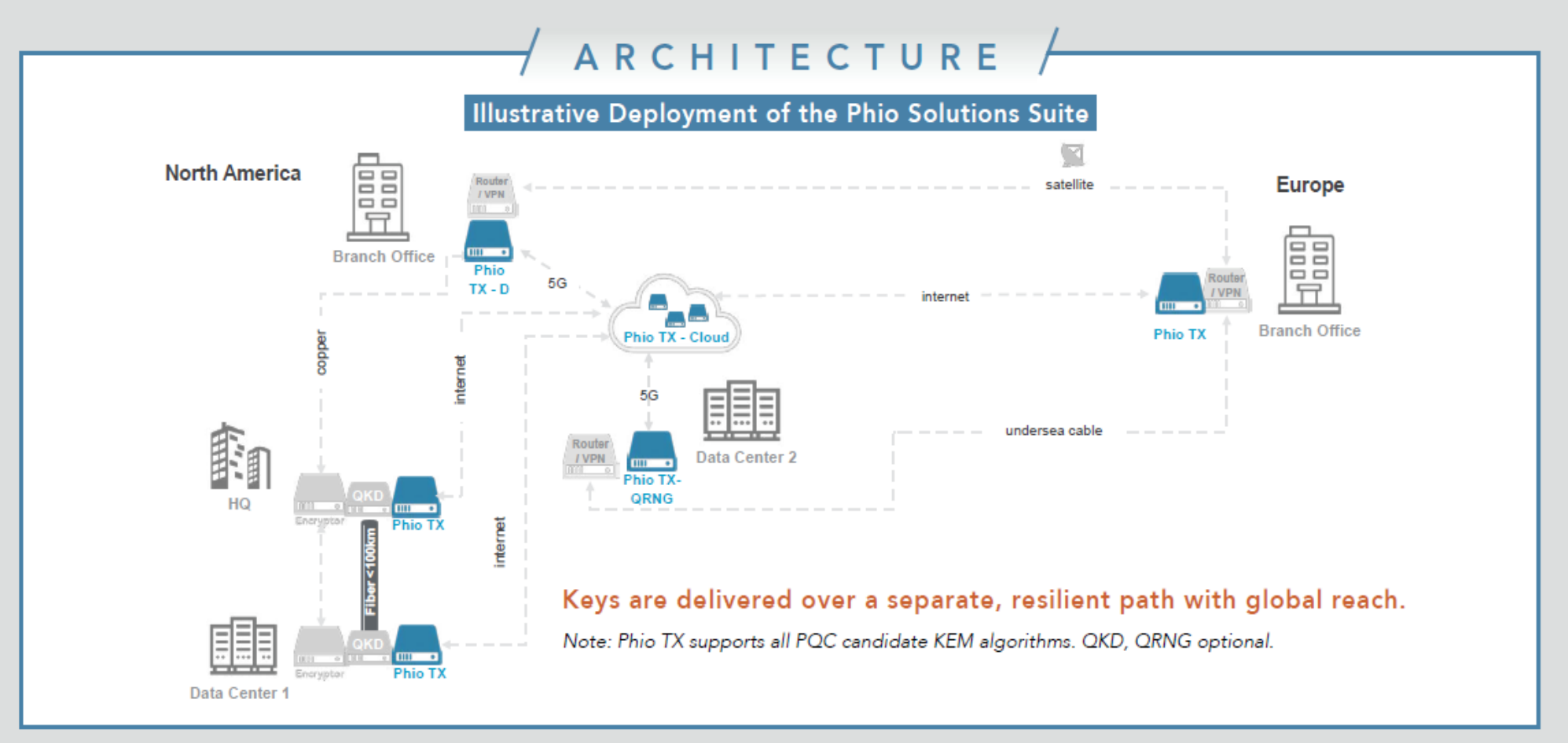
- Layer2,3 장치에 연결하여 기능 제공
- PHIO TX 또는 PHIO TXC 필요
- PHIO TX와 마찬가지로 QKD, QRNG, PQC 등 모든 방법으로 보호되는 키를 지원
- 지사용 디바이스로 원격 설치 가능

PHIO TXC

- PHIO TXC는 요청 시 대칭 암호화 키를 생성하고 한쌍의 암호화 장치에 전달하여 TLS 링크 기술을 사용하지 않고 암호화 된 채널 생성
- 다중 경로 라우팅, 로드밸런싱, 구리, 광섬유, 4G,5G,위성 등 IPv4,IPv6 지원

4. Quantum Xchange

- 종합 아키텍처



4. Quantum Xchange

- 인증 및 호환성

검증된 PQC 업체와의 협력 및 교류

보안 솔루션 부문
WORLD FUTURE
AWARDS 수상

Cyber Defense
Magazine
수상

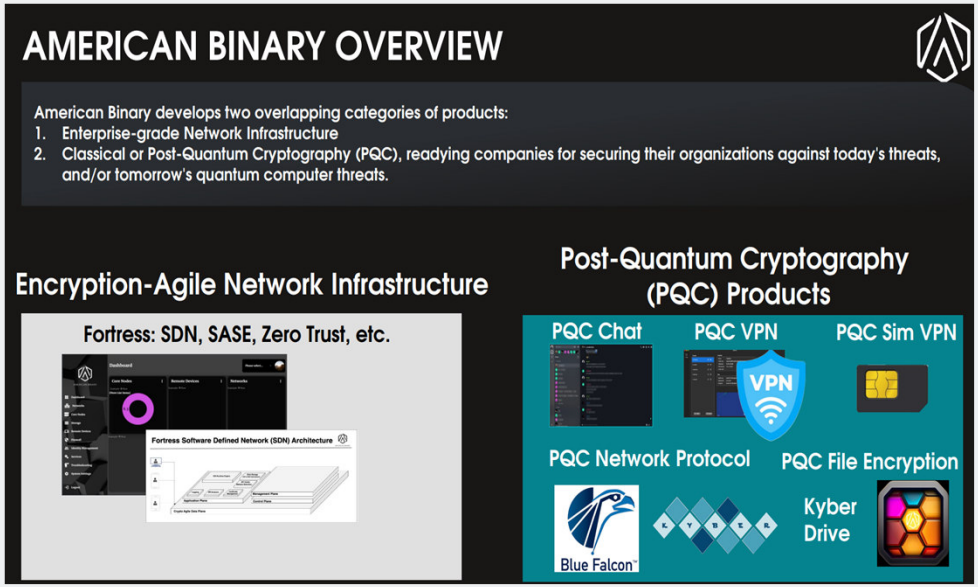
2022 Cyber Security
Global Excellence
Awards 수상

2021 Big50
스타트업 보고서
핫 스타트업 선정

제조사	네트워크 계층	암호화 기술	지원되는 모델
ADVA Optical Networking	계층 1 – 물리적	OTN/WDM 암호화 (AES-256)	o FSP 3000 커넥트가드
ciena	계층 1 – 물리적	OTN/WDM 암호화 (AES-256)	o Waveserver® 5 플랫폼
JUNIPER NETWORKS	레이어 2 – 데이터 링크	이더넷 VPN/ MACSec (AES-256)	o NFX 및 SRX 시리즈(JunOS 22.4)
THALES	레이어 2 – 데이터 링크	이더넷 VPN/ MACSec (AES-256)	o Centauris(CN9, 6 및 4 시리즈)
FORTINET	계층 3 - 네트워크	IP VPN/IPSec(AES-256)	o Fortigate 장치(FG 9, 8, 6,5,4,3 및 2 시리즈)
CISCO	계층 3 - 네트워크	IP VPN/IPSec(AES-256)	o ISR4K,ISR1K o ASR1K o CAT8500 및 CAT8300 o C8000V o CSR1000v
THALES	계층 3 - 네트워크	IP VPN/IPSec(AES-256)	o CV1000 시리즈(가상 암호기)

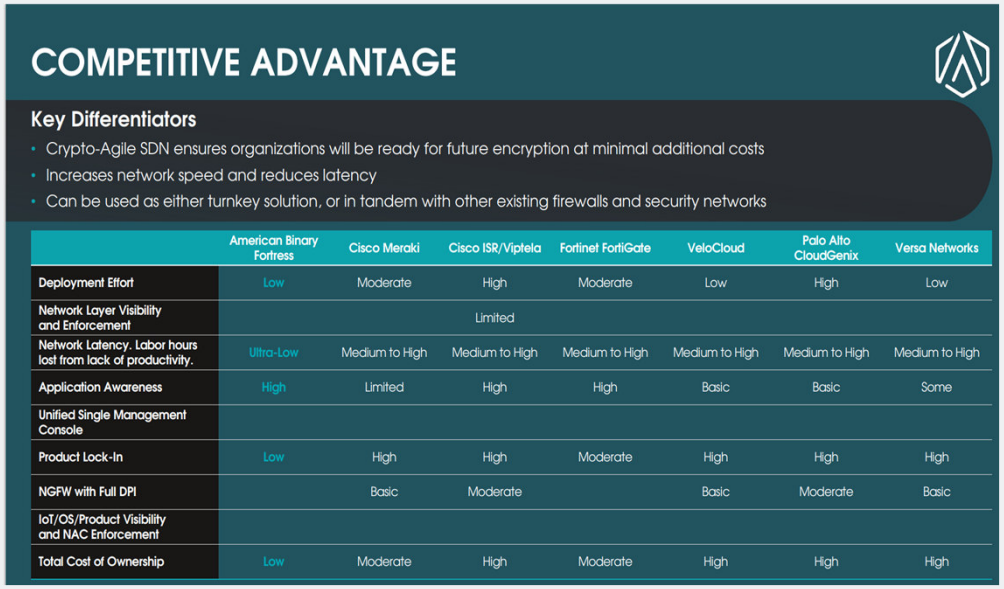
5. American Binary

제품 선정 배경



- PQC 방식에 적용되는 PQC Chat, PQC-VPN 등 기능 제공
- SDN 서비스 제공에 특화된 Fortress 제품 주력
- 휴대폰에 PQC방식의 E-Sim Card 가능 제공으로 암호화
- PQC방식으로 국방 및 헬스케어 분야에서 인상적인 효과를 제공

추진 내역



	American Binary Fortress	Cisco Meraki	Cisco ISR/Viptela	Fortinet FortiGate	VeloCloud	Palo Alto CloudGenix	Versa Networks
Deployment Effort	Low	Moderate	High	Moderate	Low	High	Low
Network Layer Visibility and Enforcement			Limited				
Network Latency. Labor hours lost from lack of productivity.	Ultra-Low	Medium to High	Medium to High	Medium to High	Medium to High	Medium to High	Medium to High
Application Awareness	High	Limited	High	High	Basic	Basic	Some
Unified Single Management Console							
Product Lock-In	Low	High	High	Moderate	High	High	High
NGFW with Full DPI		Basic	Moderate		Basic	Moderate	Basic
IoT/OS/Product Visibility and NAC Enforcement							
Total Cost of Ownership	Low	Moderate	High	Moderate	High	High	High

- 미국 본사와 수차례 화상회의를 통해 장비 기술검증과 상호 신뢰도 형성
- 국내 도입을 위해 국가정보원 보안적합성 통과를 위한 사전 항목 검토
- Client PoC 테스트 완료
- Fortress PoC 테스트 진행 예정

JIN INFRA
ICT SMART CONVERGENCE

CONTENTS

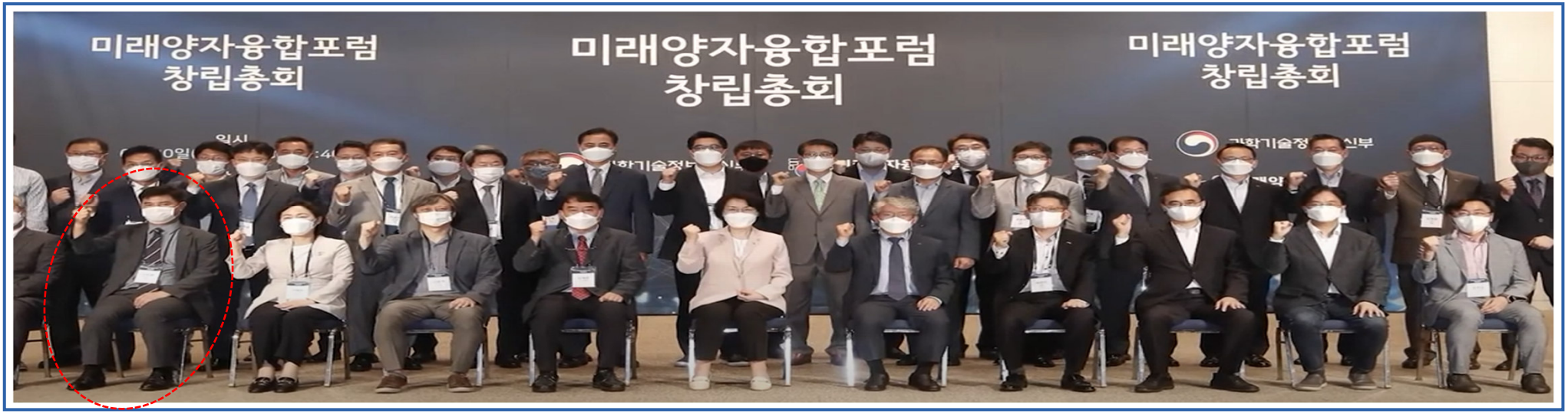
Ⅳ. 진인프라 양자 보안사업 뱡향

IV 진인프라 양자 보안사업 방향

1. 양자산업 생태계 활성화 내역

- 미래양자융합포럼 발족

- 2021년 6월 양자(통신·컴퓨팅·센서)분야의 산·학·연 교류와 양자산업 생태계 활성화를 위해 만들어진 조직
- 공동대표의장 : kt 홍경표(현 김이한 원장), KIAS 김재완 교수
- 통신대기업 : kt, skt/skb, lgu+
- 일반기업 : LG전자, 한국전력, 진인프라 등
- 공공기관 : NIA, ETRI, TTA, NSR, KIST, KRISS, IITP, NRF
- 학계 : 성균관대, 한양대, 부산대, KAST, 고려대, 서울대



IV 진인프라 양자 보안사업 방향

1. 양자산업 생태계 활성화 내역

- 미래양자융합센터 - 진인프라 MOU 체결

MoU 체결

QCI 미래양자융합센터 Future Quantum Convergence Institute

진인프라

(사)미래양자융합센터 - (주)진인프라 양자산업생태계 활성화 협력을 위한 업무협약(MoU) 체결
- 해외 진출 공동 추진 등 협력 -

보도 자료

미래양자융합센터-진인프라, 양자산업 생태계 활성화 협력

| 해외 진출 공동 추진 등 협력

과학 | 입력 :2023/08/08 20:50

한세희 과학전문기자 | 기자 페이지 구독 기자의 다른기사 보기

[사전등록] 로옴 Web 세미나(10월 18일) - DC-DC 컨버터의 EMC 대책 (제1편), 지금 등록하세요!

미래양자융합센터와 진인프라가 8일 양자산업 생태계 활성화를 위한 업무협약(MoU)을 체결했다.

미래양자융합센터는 산학연 전문가 및 기관으로 구성된 미래양자융합포럼을 운영하고 있다. 진인프라는 네트워크, 정보보안, 통신회선, 클라우드 등을 설계·구축·컨설팅 하는 ICT 전문기업으로 양자 융합기술로 확장을 추진 중이다.

두 기관은 국내 양자산업 생태계 활성화를 위해 공동으로 노력하고, 장기적으로 이를 기반으로 해외 진출을 공동 추진하기로 했다. 미래양자융합센터는 국내외 민간 및 공공 유관 기관과 협력 관계를 구축하고, 국내외 양자 분야 산학연 기관과 사업화 기회를 마련한다. 진인프라는 양자통신 분야를 중심으로 양자 분야 시장 발굴·개척, 컨설팅 등을 진행하고, 관련 제품의 설치와 구축, 기술지원, 유지보수 등 역량 확충에 주력한다.

※ 출처 지디넷코리아 기사, ZDNET

1. 양자산업 생태계 활성화 내역

양자기술 산업생태계 발전 세미나 참석

양자기술 산업생태계 발전 세미나

보도 자료

"양자센싱·양자통신분야 우리나라가 글
가능"

미래양자융합포럼, 15일 양자기술 산업생태계 발전 세미나 개최

과학 | 입력 :2023/09/15 17:00

한세희 과학전문기자 | 기자 페이지 구독 기자의 다른기사 보기

[자세히보기] 카카오클라우드 Up to 66% 초강력 할인! 초고사양, 초저가로

양자 통신과 양자 센싱 분야의 주도권 확보가 향후 양자 컴퓨팅 시장 글로벌 경쟁력의 기반이 될 수 있다고 전문가들이 입을 모았다.

미래양자융합포럼(공동의장 김재완·김이한)은 15일 서울 양재동 엘타워에서 국가 양자산업 경쟁력 강화 방안을 찾기 위한 '양자기술 산업생태계 발전 세미나'를 개최했다.

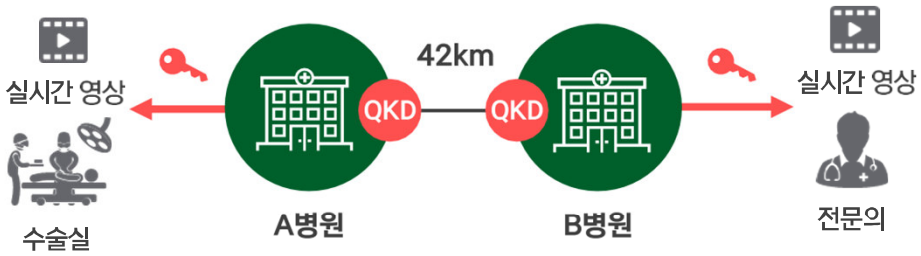
※ 출처 지디넷코리아 기사, ZDNET

1. 양자산업 생태계 활성화 내역

진인프라 양자통신 구축 사례

의료데이터(A병원 ↔ B병원)

구성도 ('21)



Quantum-실시간 의료 협진

대학병원의 영상 코덱에 양자암호키를 주입하여 수술영상을 원격지로 송출, 본원/분원 전문의와 실시간 의료 협진

※ 향후, 의과 대학생 및 인턴 등의 교육서비스로 확장 예정

공정데이터(설비시설 ↔ 관제센터)

('21)

QRNG-로봇 IoT

산업용 로봇 IoT 통신 모듈에 QRNG를 적용하여, 암호화된 데이터를 수집서버 및 관제서버로 전송, 산업용 로봇 IoT 센서와 통신하여 실시간 관리

1. 양자산업 생태계 활성화 내역

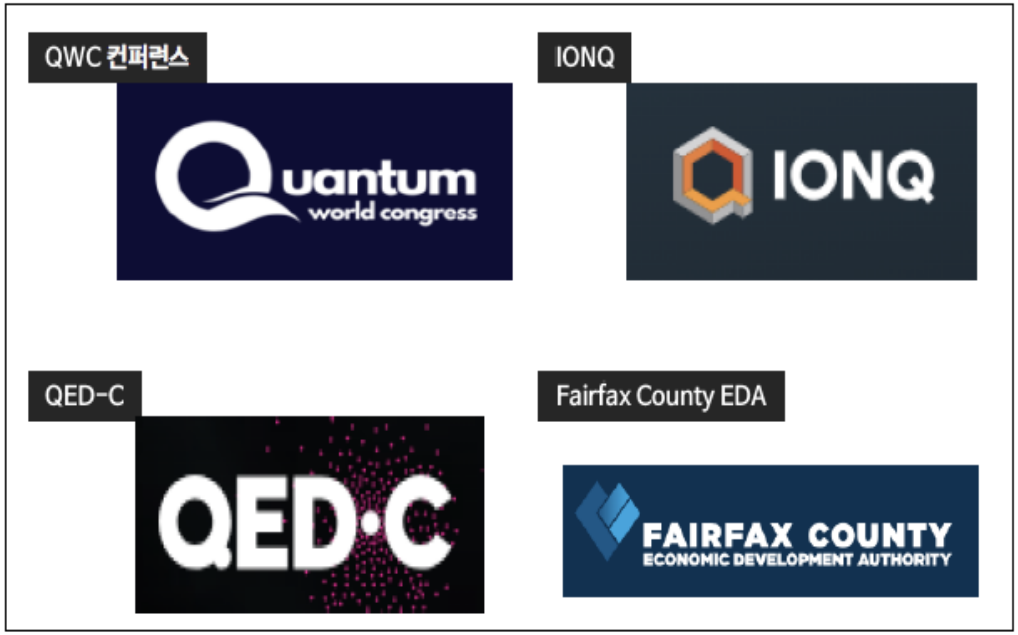
2023 글로벌 교류 프로그램 (2기)

국내 ICT 산·학·연 대상 **해외 세미나, 학술대회, 전시회 참여**를 통한 **국내 양자산업인력 글로벌 역량 강화**

2023년

- (장 소) 미국 워싱턴
- (기 간) 2023.9.25.~10.1. (5박 7일)
- (대 상) 국내 산·학·연 대표단 22명 및 관계자
- (방 문)

1) QWC 컨퍼런스 (Quantum World Congress)
2) QED-C
3) IonQ
4) Fairfax County EDA



IV 진인프라 양자 보안사업 방향

1. 양자산업 생태계 활성화 내역

개인 활동내용

- QWC 컨퍼런스 참여 및 비즈니스 미팅 진행
- (대표단 자체교류회) 3분 자유발표 준비
  - 자기소개, 참가소감 및 자유주제 발표
- (Fairfax County EDA) 소속 기업/기관 소개 준비
  - 라운드테이블?? 영문 소개 또는 한글 소개(통역사 연결)
- (기업/기관 방문) 개인 질의응답 준비 (필요시)

※ 개인 활동내용 사진촬영

개인 과제

- 참여계획서 제출

  1) QWC 컨퍼런스

  QWC 컨퍼런스 기간 동안 듣고자 하는 세션을 작성하여 제출

  2) 비즈니스 미팅

  QWC 연사 사전 탐색 후, 비즈니스 미팅 대상자 및 목적 작성
  현장에서 회의 시간 협의되면 KQIC 에서 통역 지원

- 일일보고서

  - 내용: 개인별 매일의 활동내용을 간단하게 작성
  - 분량: 1-2페이지
  - 비고: 시사점 및 사진첨부(중요!)

IV 진인프라 양자 보안사업 방향

1. 양자산업 생태계 활성화 내역

조별 활동내용

- (대표단 자체교류회_조별) 조별 자체교류회 진행
  - 전체 일정 및 개별 일정 고려하여 상호협의를 통해 장소, 방법 등 자체적으로 결정하여 진행 (9/28 추천)
  - 내용: 조별보고서를 함께 토의 및 검토 진행
- (조별 카톡방 운영)
  - 조별보고서, 인사이트, 정보 등 공유
- (기업/기관방문) 조별 질의 진행
  - QED-C, Fairfax, IonQ 방문 시 조별 질의응답 참여

※ 조별 활동내용 사진촬영 (카톡방 캡쳐)

조별 과제

- 조별보고서
  - 조별 7개 세션의 보고서 작성
  - 1개의 보고서는 2인 1조로 작성
  - 분량: 세션당 1페이지 작성
  - 비고: 별도 사진첨부
  - 조별로 조별보고서를 취합/공유 후 논의 필수

IV 진인프라 양자 보안사업 방향

1. 양자산업 생태계 활성화 내역

Quantum World Congress (2~4일차)

9/26

부트캠프

양자통신 소개

UNIVERSITY OF MARYLAND

9월 26일 화요일
오전 09:00 – 오후 12:00

양자통신에 관심있는 누구나
1인당 $49.99

4개의 큐비트를 사용한 최신 양자 오류 수정

NIST National Institute of Standards and Technology U.S. Department of Commerce

Joint Center for Quantum Information and Computer Science

9월 26일 화요일
오후 01:00 – 오후 02:30

양자 오류 정정의 5WH에
관심이 있는 누구나
1인당 $49.99

혁신 및 기업가 정신 집중 강좌: Quantum을 위한 I-Corps 소개

NSF CORPS NSF Innovation Corps

9월 26일 화요일
오후 03:00 – 오후 05:00

대상 및 비용 미정

교실 속의 양자

GEORGE MASON UNIVERSITY

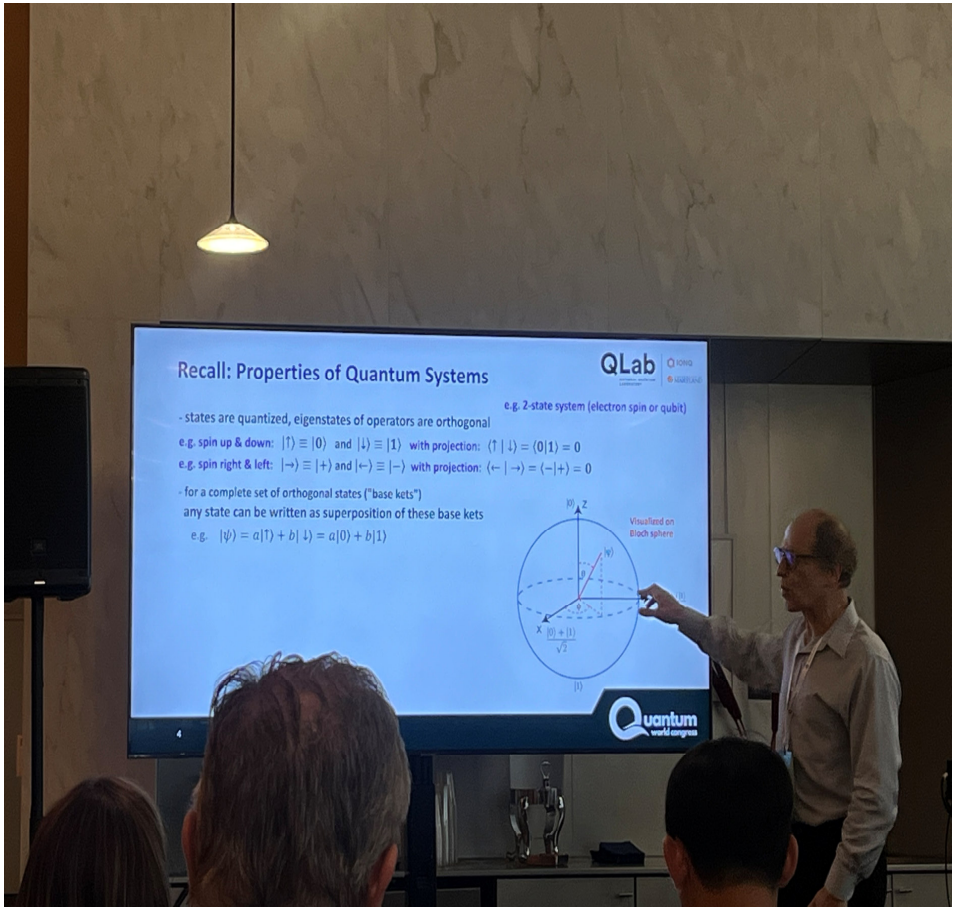
POTOMAC QUANTUM INNOVATION CENTER

9월 26일 화요일
오후 05:00 – 오후 07:00

초등, 중, 고등학교 교사(권장)
$75의 급여와 전문 개발 크레딧

해당적음

1. 양자산업 생태계 활성화 내역



1. 양자산업 생태계 활성화 내역

대표단 자체교류회 (2일차)

프로그램 개요

- (일 시) 2023.9.26.(화) 19:00~21:00(EST) ※ 프로그램 2일차
- (장 소) CAPITAL ONE HALL 內 컨퍼런스룸 ※ QWC 행사장 내 위치
- (참석자) KQIC 양자 ICT 글로벌 교류 2기 대표단 및 관계자
- (주요내용)
  - 대표단 자기소개 및 상호교류를 통한 네트워크 형성
  - NIA 양자분야 사업소개 및 성과공유
  - 대표단 양자관련 자유발표를 통한 관심사항 청취

세부 일정표

시 간	내 용	비 고
19:00~19:10('10)	환영 인사 말씀	NIA
19:10~19:30 ('20)	NIA 양자분야 사업소개 및 성과공유	NIA
19:30~20:50 ('80)	한국 산·학·연 대표단 3분 발표 ▶ 자기소개, 소속기관·기업 소개, 참가 소감 ▶ 자유주제 발표 : 최근 양자이슈, 양자기술의 방향성, 세계 양자시장에서의 한국의 역할 등 자유의견 발표	대표단 전체
20:50~21:00 ('10)	기념촬영 및 마무리	

1. 양자산업 생태계 활성화 내역

IV 진인프라 양자 보안사업 방향

1. 양자산업 생태계 활성화 내역

1. 양자산업 생태계 활성화 내역

QED-C (3일차)

프로그램 개요

- (일 시) 2023.9.27.(수) 18:00~19:30(EST) ※ 프로그램 3일차
- (장 소) CAPITAL ONE HALL
- (참석자)
  - (한국) KQIC 양자 ICT 글로벌 교류 2기 대표단 및 관계자
  - (미국) QED-C Celia Merzbacher (전임이사) 등
- (주요내용)
  - QED-C 사무국 및 관계자와 네트워킹 형성
  - 한미 양자산업생태계 동향 발표 및 기관 소개
  - QED-C 관련 개인 및 기업별 질의 응답 및 답변

세부 일정표

시 간	내 용	비 고
18:00~18:10('10)	QED-C 사무실 방문 (체크인)	
18:10~18:30('20)	QED-C 사업 소개 및 미국 양자산업 동향 발표	QED-C
18:30~18:50('20)	NIA 사업 소개 및 한국 양자산업 동향 발표	NIA
18:50~19:20('30)	질의응답	전체 참석자
19:20~19:25('5)	한미 상생협력 방안에 대한 제언	NIA · QED-C
19:25~19:30 ('5)	전체 사진촬영 및 마무리	전체 참석자

1. 양자산업 생태계 활성화 내역

1. 양자산업 생태계 활성화 내역

Fairfax county EDA (5일차)

프로그램 개요

- (일 시) 2023.9.29.(금) 10:00~13:00 (EST) ※ 프로그램 5일차
- (장 소) Fairfax County EDA(Economic Development Authority)
  (8300 Boone Boulevard Vienna,VA 22182)
- (참석자)
  - (한국) KQIC 양자 ICT 글로벌 교류 2기 대표단 및 관계자
  - (미국) Fairfax County EDA 관계자, U of George Mason 등
- (주요내용)
  - Fairfax County EDA 사업소개
  - George Mason University Quantum Center 소개
  - KQIC 참가단 산업계 소개

세부 일정표

시 간	내 용	비 고
10:00~10:15 ('15)	Fairfax county EDA 방문 및 체크인	
10:15~10:45 ('30)	NIA 소개 및 Fairfax County EDA 사업소개	NIA Fairfax
10:45~11:15 ('30)	George Mason University Quantum Science and Engineering Center 소개	U of George Mason
11:15~11:45('30)	What Is Soft Landing	Embark
11:45~12:00('15)	미국 현지 사업 경험 사례 공유	Korean Company
12:00~13:00('60)	KQIC 참가단 소개 점심 및 라운드테이블(Q&A)	전체

1. 양자산업 생태계 활성화 내역

1. 양자산업 생태계 활성화 내역

IonQ (5일차)

프로그램 개요

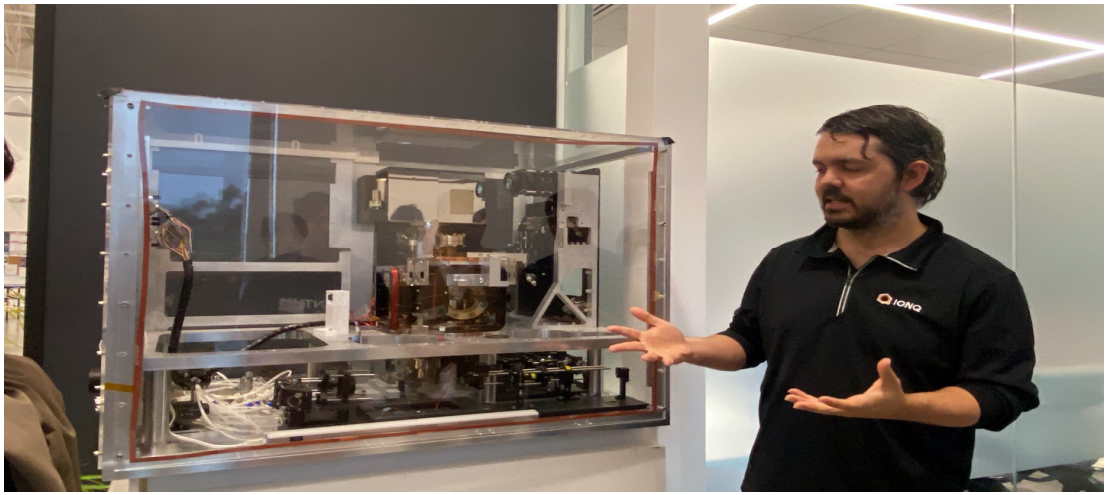
- (일 시) 2023.9.29.(금) 15:00~17:00 (EST) ※ 프로그램 5일차
- (장 소) IonQ (4505 Campus Drive, College Park, MD, 20742, US)
- (참석자)
  - (한국) KQIC 양자 ICT 글로벌 교류 2기 대표단 및 관계자
  - (IonQ) 김정상 교수 등
- (주요내용)
  - IonQ 사업소개
  - IonQ 연구소 및 기관 투어
  - KQIC 대표단 질의 및 토의

세부 일정표

시 간	내 용	비 고
15:00~15:15 ('15)	Introduction	
15:15~15:45 ('30)	Company Introduction for IonQ	
15:45~16:15 ('30)	Any discussions from the Quantum Industry Delegation	전체
16:15~16:55 ('40)	IonQ Facility Tour	IonQ
16:55~17:00('5)	기념촬영 및 마무리	

IV 진인프라 양자 보안사업 방향

1. 양자산업 생태계 활성화 내역



2. 양자산업 생태계 활성화 방향

저비용 고효율 방식의 사업사업 확대 추진

다양한 방식의 양자 암호통신 인프라 구축
→ QKD/PQC에서 Hybrid 방식으로 구축 및 실증

1. 1:1 방식에서 1:N, N:N 방식으로 사업 확대
2. Hybrid 방식으로 장비 구성하여 투자비 절감

외산벤더 도입을 통한 기술경쟁력 확보

양자암호통신 글로벌 벤더와의 협력
→ 외산벤더와 경쟁을 통해 국내기술력 향상

1. 다수의 글로벌 QKD, PQC 벤더 등과 협력
2. 국내 기관 인증을 통한 해외 기술력 파악 및 습득

JIN INFRA

Total 컨설팅 전담사 운영

양자 암호통신 활성화 국내 컨설팅 주관
→ 24시간 365일 양자분야 컨설팅 제공

1. 망설계, 구축, 운용 등 관심고객 대상 발굴 종합컨설팅 제공
2. 유,무선, 클라우드 및 전송/네트워크/보안 분야 기술지원

홍보 및 교육 강화

언론, 미디어 등 다양한 매체를 통한 홍보
→ 홍보를 통한 양자 중요성 피력

1. 초,중,고 대학교 및 전 국민들의 양자에 대한 중요성 홍보
2. 양자주간, 양자의날 등 부스 운영 및 언론, 홍보 주기적 추진


Thank you