

해외출장 결과보고

MobiSec 2024 워크숍 참석을 위한 일본 해외출장 결과보고

2025. 1.

I. 출장 개요

□ 개요

- (출장기간) 2024. 12. 16.(월) ~ 2024. 12. 19.(목)
- (장 소) 일본 삿포로
- (출장자) 이음5G사업팀 손세일, 박연규
- (출장목적) 「양자보안 기반 5G특화망 기기 식별 기술 및 시험검증 기술개발」 관련 ①5G특화망 보안 기술 동향 조사를 위한 MobiSec 2024 참석 및 ②성과점검 워크숍 참석 등

□ 주요일정

일 자	출발지	도착지	업무수행내용	비 고
12.16.(월)	인천	일본 (삿포로)	○ 나주 → 인천국제공항 이동 ○ 인천국제공항 → 일본(삿포로) 이동	
12.17.(화)	일본 (삿포로)		○ MobiSec 2024 참가 - 양자보안 기술 동향 조사·분석	MobiSec 2024
12.18.(수)			○ 5G 보안 및 양자보안 기술 세미나(대만) ○ 6G 보안 기술 동향 세미나(일본) ○ 5G특화망 기기식별 사업 성과점검 ○ 5G특화망 국제공동연구 아이템 발굴	TTA 워크숍
12.19.(목)	-	인천	○ 5G특화망 전문가 네트워킹 ○ 일본(삿포로) → 인천국제공항 → 나주 이동	

Ⅱ. MobiSec 2024 주요내용

□ 회의 개요

- 기간 및 장소 : 2024. 12. 16. (월) ~ 19. (목), 일본 삿포로
- 회의 내용 : 모바일 인터넷 보안과 사이버 보안 분야에서 직면한 보안 문제의 해결을 위한 산·학·연 연구내용 발표 등
- 참가자: 한국, 일본, 중국, 대만, 이탈리아, 폴란드, 스페인, 터키, 덴마크, 오스트리아, 인도, 태국 등 18개국에서 약 350명 참가

□ 주요 내용








① MobiSec 2024




- (네트워크 보안) 차세대 네트워크와 분산 컴퓨팅(edge/cloud) 기술의 확대에 따라 상호 연결성이 증가하면서, 네트워크의 보안, 신뢰성 등에 대한 중요성이 증가
 - (유럽) B5G/6G 보안을 중점으로 연구하는 프로젝트(RIGOUROUS)를 통해 차세대 모바일 네트워크, 장치, 컴퓨팅 인프라 및 서비스에서 발생하는 보안 등 위험 식별 및 해결
 - (일본) ICT 연구기관(NICT)에서 사이버 보안 관련 연구를 진행 중이며, 최근 발생하고 있는 DoS/DDoS 사건의 대응 방안 소개

구분	DoS(Denial of Service)	DDoS(Distributed Denial of Service)
공격 소스	단일 시스템	다수의 분산된 시스템
공격 규모	상대적으로 작음	대규모
방어 난이도	상대적으로 낮음	탐지와 방어가 복잡함
효과 범위	특정 네트워크 또는 시스템	광범위한 네트워크 또는 서비스

② 5G특화망 국제공동연구 아이템

- (교류회) 5G특화망용 양자보안 관련 공동 연구 아이템 발굴을 위한 연구내용 발표를 통한 국제(일본, 이탈리아, 대만, 인도, 한국) 협력 추진

번 호	발표자	소속/국가	주 제	비 고
1	Alessio Merlo 교수	CASD /이탈리아	국제 공동 연구를 위한 EU 지원 프로그램	
2	이옥연 교수	국민대 /대한민국	양자 보안 R&D 현황	
3	김용대 교수	KAIST /대한민국	이동통신 보안 연구 현황	
4	신성한 박사	AIST /일본	AIST 사이버-물리보안 연구센터(CPSEC) 소개	
5	Shih-Hao Hung 교수	국립타이완대학 /대만	효율적이고 신뢰로운 AI	
6	전숙현 팀장	TTA /대한민국	이음5G eqSIM 연구개발 현황 (국민대, KCA, 라임CSI, 이루온 공동)	
7	박종근 실장	ETRI /대한민국	ETRI 정보보호본부 소개	

번 호	발표자	소속/국가	주 제	비 고
8	Kiji Nakao 교수	NICT /일본	한-일 사이버보안 국제협력	
9	C. Pandu Rangan 교수	Indian Institute of Science /인도	양자컴퓨팅 보안 및 고급 암호	
10	Junji Shikata 교수	Yokohama National University /일본	양자내성암호 및 B5G/6G 보안	

③ QS-5GNPN 2024 (TTA Workshop)

- (암호 기술의 역사) 2차 세계대전에서 독일 에니그마(Enigma) 암호의 해독에 컴퓨터를 활용하면서 암호 기술의 변혁이 시작됨
 - 이에 따라, 컴퓨터를 이용한 공격에도 안전성을 높이기 위해 수학적 난제를 기반한 공개키 암호가 개발되었으며, 이게 현재의 암호 기술임
 - (RSA) 1977년 Ronald Rivest, Adi Shamir, Leonard Adleman이 개발하였으며, 소인수분해 문제의 계산적 어려움에 기반함
 - 암호화와 복호화에 서로 다른 키를 사용하고 2,048 bits 이상의 키를 사용하면 현재의 컴퓨터 성능으로는 해독이 어려움
 - (ECC) 1990년대 타원 곡선 암호(ECC, Elliptic Curve Cryptography)가 개발되었고, 타원 곡선 방정식에서 정의된 점 간의 연산 어려움에 기반함
 - RSA보다 더 짧은 키로 강력한 보안을 제공하며 계산 자원이 제한된 환경에서 더욱 유리함

- **(PQC 등장 배경)** 양자컴퓨터의 발전으로 인해 RSA, ECC와 같은 전통적인 공개키 암호 알고리즘의 안정성이 위협받음
 - NIST(미국 국립표준기술연구소)에 따르면, 앞으로 10~15년 사이에 가장 많이 사용되고 있는 RSA-2048이 24시간 이내에 해독될 전망이 우세함
- **(PQC 정의)** 기존 공개키 암호와 같이 수학적 난제에 기반하지만, 양자컴퓨터로도 해독이 힘든 난제를 활용하여 설계된 양자내성 암호(PQC, Post Quantum Cryptography)
 - 기존 공개키 암호의 난제는 시간 측면에서 효율적인 해결 알고리즘인 'Shor 알고리즘'이 알려져 있음
 - 반면, PQC는 효율적 해결 알고리즘이 알려지지 않은 수학적 난제에 기반을 두고 개발됨
- **(패러다임 전환)** PQC로의 전환을 위해 각국에서는 기존 암호 기술을 한시적으로 허용하면서, 신규 기술/표준이 제품에 적용 되도록 정책을 지원하고 있음
 - **(미국)** '21년 8월, 「Migration to Post-Quantum Cryptography」를 발표하여, 암호 모듈, 암호 라이브러리, 응용 제품, 암호 코드, 통신프로토콜 순으로 PQC 전환을 계획함
 - **(유럽)** '22년부터 PQC 전환 과제*를 추진하여 표준화, 인증, 솔루션 구현 등 PQC 전환을 단계적으로 진행 중임
 - * Transition towards Quantum-Resistant Cryptography, TOPIC ID: HORIZON-CL3-2022-CS-01-03
 - **(프랑스)** ANSSI(사이버보안국)는 PQC로의 전환을 3단계로 구분하여 양자컴퓨팅에 암호 안전성을 확보하고자 함

구 분	주요 내용
1단계 (현재)	양자내성암호 전환 준비 단계로 양자내성암호의 안전성에 집중
2단계 (2025-2030)	양자내성 안전성이 없는 제품들의 조달을 점진적으로 중단
3단계 (2030+)	양자내성 안전성을 기본 특성으로 설정

- (PQC 개발 현황) 2006년 PQCrypto 학회가 설립되면서 개발 논의가 본격화되었고, '16년에 시작된 NIST의 PQC 공모사업의 3단계에 걸친 평가 결과 4개의 암호 알고리즘이 선정됨
- (국외) 키 교환과 암호화에 CRYSTALS-Kyber 1종, 전자서명에 CRYSTALS-Dilithium, Falcon*, SPHINCS+ 3종

구 분	키 교환/암호화		전자서명	
	선정	대안 후보	선정	대안 후보
격자 기반 (Lattice-based)	CRYSTALS-Kyber , NTRU, SABER	NTRU-Prime, FrodoKEM	CRYSTALS-Dilithium , Falcon	
코드 기반 (Code-based)	Classic-McEliece	BIKE, HQC		
다변수 기반 (Multivariate-based)			Rainbow	CeMSS
해시 기반 (Hash-based)				Picnic SPHINCS+
기타 (Isogeny-based)		SIKE		

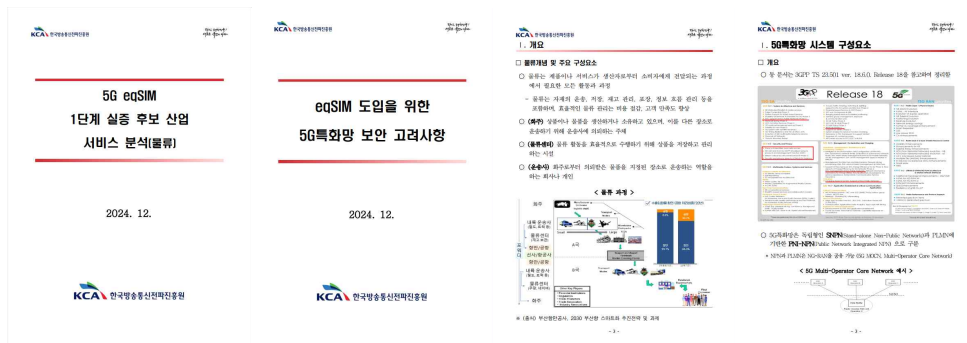
- (국내) 양자내성암호연구단(KpqC) 공모 1라운드에서 키 교환과 암호화에 4종, 전자서명에 4종이 2라운드에 진출함

1라운드 (’23년 12월 기준)	키 교환/암호화	전자서명
격자 기반	NTRU+, SMAUG+TiGER	AlMer , GCKSign, HAETAE , NCC-Sign , Peregrine, SOLMAE
코드 기반	IPCC, LayeredROCK, PALOMA, REDOG	Enhanced-pqsigRM
다변수 기반		MQ-Sign
기타		FIBS

- (보안 위협) 5G 네트워크 보안 관련 주요 위협 요소에는 스푸핑(Spoofing), DoS 공격, 도난 및 도청에 의한 기기 악용, 물리적 취약성이 있음
 - (스푸핑) IoT 장비, 스마트폰 등 종단 장치(Edge device)를 통해 무단 로그인하여 악성코드를 배포하여 기밀 정보 유출
 - (대응방안) 종단 장치의 암호 설정 규칙 규정·운용, 정기적인 장치 취약성 및 악성코드 검사, 진정성(Authenticity) 보증 등
 - (DoS) 악성코드 등에 의해 무단 탈취된 종단 장치에서의 대량 시그널링 송신으로 네트워크 과부하 발생 및 시스템 성능 저하
 - (대응방안) 각 장치(기지국, 코어)에서 처리 가능한 시그널링량의 임계치 설정 및 초과된 시그널링이 발생한 경우는 재접속 요청 거부
 - (도난/도청) 장비 접근 권한 관리 부실 및 보안성이 낮은 암호 알고리즘 사용으로 인한 도난 및 도청
 - (대응방안) 장치의 보수·운용에 대한 권한을 기록 및 관리하고 암호 알고리즘 및 암호키의 키 길이 관련 정책 규정



- (5G특화망 기기식별 사업 성과점점) '24년 실적 목표인 기술문서 2건, 학술대회 1건, 홍보 1건 모두 달성하였고, 사업비 집행률은 92%
- (기술문서) PQC 지원 eqSIM의 실증을 위한 후보 산업 서비스 분석(물류)과 eqSIM 도입 시 고려해야 할 5G특화망 보안요소 분석



- (학술대회 논문 발표 실적) 이음5G망 구축 시, 망 구조, 구성요소, 단말 인증 과정에서의 보안 고려사항에 관한 논문 1건 발표

Tuesday, 17th December 2024			
Time	Palace Ball Room (East)	Palace Ball Room (West)	Crown Room (Online)
09:00 ~ 10:30 (1H 30M)	Session 1A 5G and RAN Security Chair: Moohong Min	Session 1B AI-driven Security (I) Chair: Younghan Lee	Session 1C Convergence Security Chair: Bonam Kim
10:30 ~ 10:45	Break (15M)		
10:45 ~ 12:00 (1H 15M)	Session 2A Cryptography and Authentication Chair: Kouichi Sakurai	Session 2B Malware and Vulnerability Analysis Chair: Dooho Choi	Session 2C Cryptography and Authentication Chair: Bonam Kim
12:00 ~ 13:40	Lunch – Complement of MobiSec conference (1H 40M)		
13:40 ~ 14:00 (Opening)	Opening Remarks by General Chair : Kiwook Sohn (SEOULTECH, South Korea)		
	Welcome Address : Goichiro Hanaoka (AIST, Japan)		
	Program Overview : SeongHan Shin (AIST, Japan)		
14:00 ~ 15:00 (1H)	Keynote 1 (Chair: Alessio Merlo (CASD, School of Advanced Defense Studies, Italy)) Prof. Antonio Skarmeta (University of Murcia, Murcia, Spain) Challenges on Security for future 6G networks		
15:00 ~ 15:15	Break (15M)		
15:15 ~ 16:15 (1H)	Special Session A (SS-SECON 1) Chair: Antonio Skarmeta	Session 3B Cryptography and Cyber Security Chair: SeongHan Shin	Session 3C Image and Video Security Chair: Philip Virgil Astillo
16:15~ 16:30	Break (15M)		
16:30 ~ 18:00 (1H 30M)	Special Session B (SS-SECON 2) Chair: Pedro Martinez-Julia	The 2024 MobiSec Workshop	Session 4C AI based Security Chair: Seongmin Park
Time	Wednesday, 18th December 2024		
09:00 ~ 10:30 (1H 30M)	Session 5A Cyber Crime & Security Policy Chair: Haehyun Cho	Session 5B Mobility Security Chair: Kiwoong Park	TTA eqSIM Project Workshop 1
10:30 ~ 10:45	Break (15min)		
10:45 ~ 12:00 (1H 15M)	Session 6A Post Quantum Cryptography Chair: Hyungrok Jo	Session 6B Emerging Techniques I Chair: Jungmin Kang	TTA eqSIM Project Workshop 2
12:00 ~ 13:30	Lunch – Complement of MobiSec conference (1H 30M)		
13:30 ~ 14:30 (1H)	Keynote 2 (Chair: Fang-Yie Leu (ThungHai University)) Prof. Koji Nakao (NICT & Yokohama National University, Japan) NICT's Cyber Security Research: Japan's ICT Research Institute's Global Cyber Security Initiatives and Research Introduction on Monitoring, Analysis and Mitigation of DoS/DDoS Attacks		
14:30 ~ 15:00	Break (30M)		
15:00 ~ 16:15 (1H 15M)	Special Session (Formal Verificaion) Chair: Jiyeon Kim	Session 7B Communication & Network Security Chair: Taek Young Youn	SEOULTECH Air Gap Workshop
16:15 ~ 16:30	Break (15M)		
16:30 ~ 18:00 (1H 30M)	Poster Session (Offline)		Global Research Collaboration Forum
19:00 ~ 21:00	Banquet – Complement of MobiSec conference (1H)		
Time	Thursday, 19th December 2024		
09:00 ~ 10:15 (1H 15M)	Session 8A AI-driven Security (II) Chair: Jungsoo Park	Session 8B Emerging Tehcnques (II) Chair: Cheoljun Park	Session 8C Cyber Threat Response Chair: Chan-Guk Jang
10:15 ~ 10:30	Break (15M)		
10:30 ~ 12:00 (1H 30M)	Session 9A Cryptographic Applications and Analysis Chair: Yuntao Wang	Session 9B Cyber Threat Detection Chair: Seongmin Kim	Session 9C 5G Security Chair: Gaurav Choudhary
12:00 ~ 13:30	Break (1H 30M)		
13:30 ~ 15:30 (2H)	The 2024 International Workshop on Intelligent Software Engineering (ISE 2024) Chair: Jiyeon Kim (Gyeongsang National University, South Korea)		
15:30 ~ 16:00	Break (30M)		
16:00 ~ 17:00 (1H)	Asia Academic – Industry Cyber Security Insight Hour		
Time	Friday, 20th December 2024		
09:00 ~ 11:00 (2H)	Roundtable on Security Challenges in the 6G, Quantum, and AI Era		

붙임2

QS-5GNPN 2024 워크숍 프로그램

□ 프로그램(안)

시간	세부내용	비고
08:00~09:00	과제 소개 및 추진 실적 및 계획 논의 - 기관별 24년 과제 추진 실적 - 25년 추진계획 논의	전체 참석자
09:00~12:00	5G 보안 및 양자보안 기술 세미나 - 5G security and quantum security technology	대만 동해대 (Prof. Fang-Yie Leu)
12:00~13:00	Lunch Break	
13:00~16:00	6G 보안 기술 동향 세미나 - 6G Security Technology Trend	일본 요코하마국립대 (조형록 교수)
16:00~17:00	컨소시엄 참여기관별 세부 진행상황 논의 - 5G 특화망 기반 양자보안기술 관련 전체 현안 논의 - 5G 특화망 스마트 공장 및 물류 현장 실증 현황 - 5G Vertical Standard 논의 - 5G 특화망 정부 정책 추진 현황 - 양자 보안 모듈 적용 기술 및 표준화 현황	전체 참석자
17:00~18:00	컨소시엄 참여기관별 협력 필요 사항 논의 - 양자내성암호를 수용하는 기기 인증서 발전 방향 - 쉴드박스형태의 특화망 RU 설치 방안 - 국내용 eSIM Remote SIM Provisioning <u>프로토콜</u>	TTA-국민대-라임
		이루온-국민대
		TTA-국민대-KCA