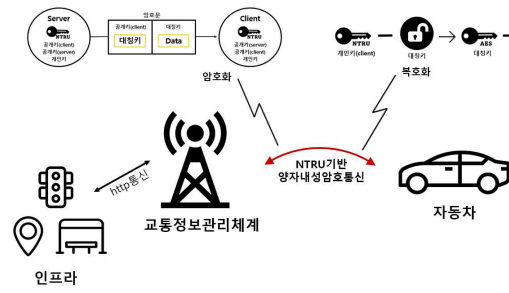


# 2021 한이음 공모전 개 발 보 고 서

2021. 8. 29

프로젝트명	국문	Quantum-Safe 기술을 이용한 자율 주행 자동차와 차세대 교통정보체계 (V2X)의 안전한 연동에 필요한 보안 모바일 망 서비스 구현
	영문	Implementation of secure mobile network services for secure interworking of autonomous vehicles and next-generation traffic information systems (V2X) using Quantum-Safe technology
작 품 명	PQC Mobility Service	

# 요 약 본

작품 정보		
프로젝트명	국문	Quantum-Safe 기술을 이용한 자율 주행 자동차와 차세대 교통정보체계(V2X)의 안전한 연동에 필요한 보안 모바일 망 서비스 구현
	영문	Implementation of secure mobile network services for secure interworking of autonomous vehicles and next-generation traffic information systems (V2X) using Quantum-Safe technology
작품명	PQC (Post-Quantum Cryptography)	
작품 소개	차세대 교통정보체계(V2X)에 강화된 보안 모바일 서비스를 위해 현 암호화 기술방식에 NTRU기반 양자내성암호기술을 적용하여 양자컴퓨팅 수준 공격에도 안전한 강도 구현	
작품 구성도	 <p>The diagram illustrates the system architecture for secure V2X communication. It shows a Server (Quantum-Safe Cryptography, Quantum-Safe Key) and a Client (Quantum-Safe Cryptography, Quantum-Safe Key) connected via a secure channel. The Server sends Data to the Client, which is then encrypted (암호화) and transmitted to the Client. The Client then decrypts (복호화) the data. The Client is also connected to a Vehicle (자동차) via a secure channel. The Vehicle is connected to a Traffic Information Management System (교통정보관리체계) via a secure channel. The Traffic Information Management System is connected to an Infrastructure (인프라) via a secure channel. The Infrastructure is connected to the Vehicle via a secure channel. The diagram also shows the process of encryption and decryption using NTRU-based quantum-resistant cryptography.</p>	
작품의 개발배경 및 필요성	<ul style="list-style-type: none"> <li>▶ C-ITS/자율주행자동차, 기업의 재택/이동/원격 근무 시 필요한 5G Network Mobility 서비스는 해킹/하이재킹 등에 안전하게 이용될 수 있어야 함</li> <li>▶ 양자 컴퓨팅(Quantum Computing)이 도입된다면, 현재의 암호화 기술 기반 보안 강도는 컴퓨팅 성능의 발달 상황에서는 개선 및 강화가 요구되고 있음</li> <li>▶ 자동차(통신 모듈, 라즈베리파이)와 차세대 교통정보체계(V2X)의 안전한 연동에 필요한 보안 모바일 망 서비스 구현을 목표함</li> </ul>	
작품의 특징점	<ul style="list-style-type: none"> <li>▶ 양자 난수 기반 암호화(NTRU 알고리즘 사용) 동작 구현</li> <li>▶ 하이브리드 암호화 시스템을 통해 암호문 생성</li> <li>▶ 양자 컴퓨터를 대비한 안전하고 높은 암호 수준의 통신이 가며, 간소화된 모델을 통해 양자 암호 통신 과정을 볼 수 있음</li> <li>▶ IoT 통신 모듈을 활용한 도로 인프라(신호등, 정류장, GPS) 데이터 수집 및 처리</li> </ul>	
작품 기능	<ul style="list-style-type: none"> <li>▶ 교통정보체계 <ul style="list-style-type: none"> <li>- 인프라 데이터 수집 및 저장</li> <li>- 키 생성 및 교환</li> <li>- 메시지 암호화 및 전송</li> <li>- 유저 인터페이스</li> </ul> </li> <li>▶ 인프라(신호등, 정류장, GPS) <ul style="list-style-type: none"> <li>- 각 모듈 값 수집</li> <li>- 값 정보 데이터 처리 및 서버로 전송</li> </ul> </li> <li>▶ 자동차 <ul style="list-style-type: none"> <li>- 키 생성 및 교환</li> <li>- 암호문 복호화</li> <li>- 유저 인터페이스</li> <li>- 시리얼 통신</li> <li>- 라인 트레이싱</li> <li>- 모터 동작</li> </ul> </li> </ul>	
작품의 기대효과 및 활용분야	<ul style="list-style-type: none"> <li>▶ C-ITS(협력 기능형 교통 체계)를 구축하기 위한 기본 토대가 됨</li> <li>▶ V2X 통신으로 운전자나 차량 탑승자의 안전 보장</li> <li>▶ 양자 컴퓨터 해킹 예방 및 NTRU 알고리즘에 관한 심화 연구에 도움</li> <li>▶ 다음 양자 내성 암호 기반 교통관리체계의 선행연구가 됨</li> </ul>	

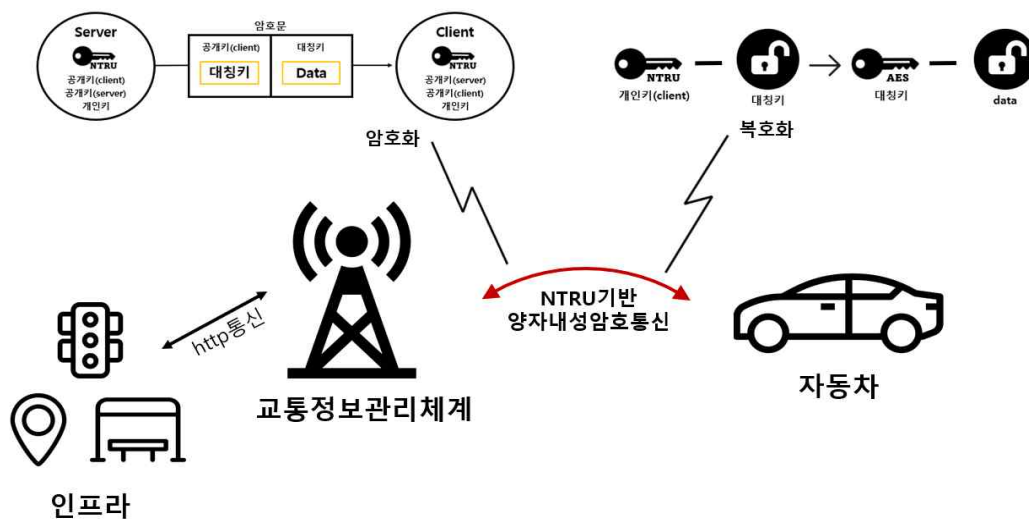
# 본 문

## I. 작품 개요

※ 평가항목 : 기획력 (필요성, 차별성)

### 1. 작품 소개

#### 1) PQC (Post-Quantum Cryptography)



- 안전성이 가장 뛰어난 양자 내성 암호 NTRU 알고리즘 방식을 적용한, 차세대 하이브리드 암호화 교통정보체계(V2X) 보안 모바일 망 서비스를 구현하는 작품

#### 2) 기획 의도

- C-ITS/자율 주행 자동차, 기업의 재택/이동/원격 근무 시 필요한 5G Network Mobility 서비스는 해킹/하이재킹 등에 안전하게 이용될 수 있어야 함
- 양자 컴퓨팅(Quantum Computing)이 도입된다면 현재의 암호화 기술 기반 보안 강도는 컴퓨팅 성능의 발달 상황에서는 개선 및 강화가 요구되고 있음
- 자동차(통신 모듈, 라즈베리파이)와 차세대 교통정보체계(V2X)의 안전한 연동에 필요한 보안 모바일 망 서비스 구현을 목표함

#### 3) 작품 내용

- 양자 내성 암호 NTRU 알고리즘 방식을 적용한 하이브리드 암호화 시스템 구축
- IoT 통신 모듈을 활용한 도로 인프라(신호등, 정류장) 데이터 수집 및 처리
- 라인트레이서의 기능을 활용한 자율 주행 자동차 구현

## 2. 작품의 개발 배경 및 필요성

### 1) 개발 배경

- 최근 양자 컴퓨팅 기술의 발달로 인한 대규모 양자컴퓨터의 실현은 현재 보안 시스템 전반에 사용되고 있는 공개키 암호시스템에 위협이 될 것으로 예상되므로 안전성을 보장받을 수 있는 양자 내성 암호로의 전환은 필수적임
- 암호의 유형으로는 격자 기반 (Lattice-based), 코드 기반 (Code-based), 다변수 기반 (Multivariate-based), 해시 기반 (Hash-based), Isogeny기반으로 나누어짐
- 격자 기반 암호인 NTRU는 NIST가 진행 중인 양자 내성 암호 공모 사업의 3라운드 최종 후보에 선정된 격자 기반 암호 중 하나
- NTRU는 동일한 안전성을 제공하는 다른 최종 후보들과 비교하여 KEM 과정에서 전달해야 하는 키와 암호문의 크기가 작다는 점에서 효율성과 안전성이 검증됨

### 2) 목적 및 필요성

- C-ITS/자율 주행 자동차, 기업의 재택/이동/원격 근무 시 필요한 5G Network Mobility 서비스는 해킹/하이재킹 등에 안전하게 이용될 수 있어야 함
- 양자 컴퓨팅(Quantum Computing)이 도입된다면, 현재의 암호화 기술 기반 보안 강도는 컴퓨팅 성능의 발달 상황에서는 개선 및 강화가 요구되고 있음
- 자동차(통신 모듈, 라즈베리파이)와 차세대 교통정보체계(V2X)의 안전한 연동에 필요한 보안 모바일 망 서비스 구현을 목표함

## 3. 작품의 특징 및 장점

### 1) 특징 및 장점

- 난수 기반 대칭키 암호화 동작 구현 (Transmitter ~ Receiver)
- 하이브리드 암호화 시스템을 통해 암호문 생성
- 양자 컴퓨터를 대비한 안전하고 높은 암호 수준의 통신이 가며, 간소화된 모델을 통해 양자 암호 통신 과정을 볼 수 있음
- 라인트레이서의 기능을 활용한 자율 주행 자동차 구현
- IoT 통신 모듈을 활용한 도로 인프라(신호등, 정류장) 데이터 수집 및 처리

### 2) 기존 교통정보체계 망 서비스와의 차별성

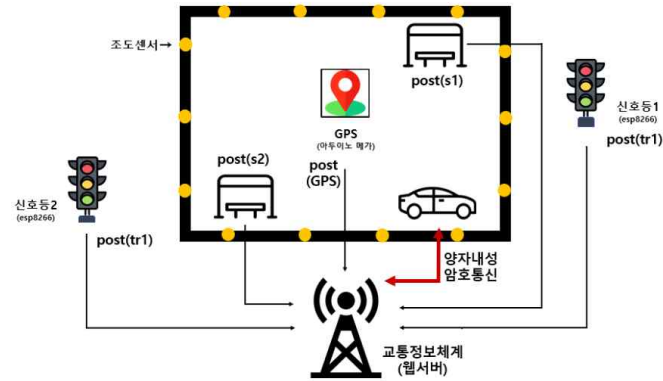
- 미국 국립표준기술연구소 NIST가 진행한 양자 내성 암호 공모 사업의 3라운드 최종 후보에 선정된 격자 기반 암호 중 하나인 NTRU 알고리즘을 사용함으로써 높은 효율성과 안전성 확립
- 하이브리드 암호시스템을 적용한 차세대 보안 통신 서비스 구축
- HTTP 통신이 아닌, Web Socket을 사용한 통신

## II. 작품 내용

※ 평가항목 : 기술력 (기능구체성, 난이도, 완성도)

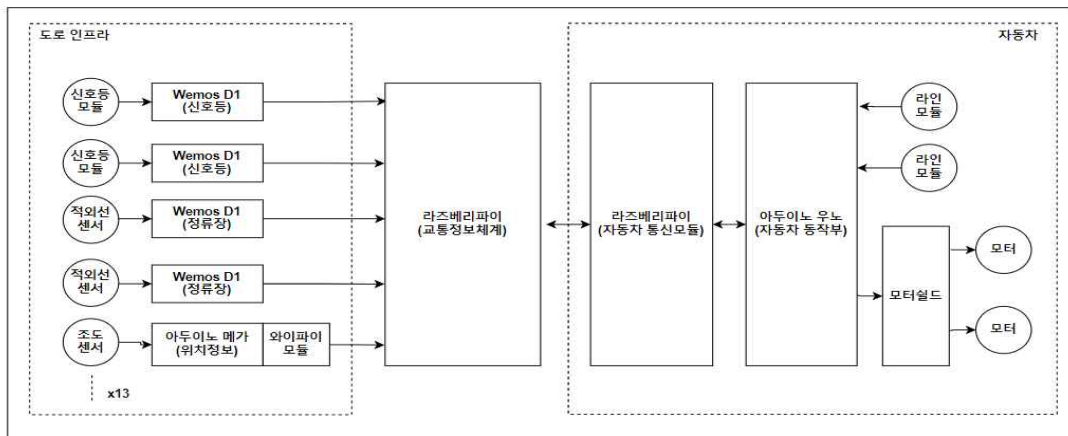
### 1. 작품 구성도

#### 1) 전체 구성도

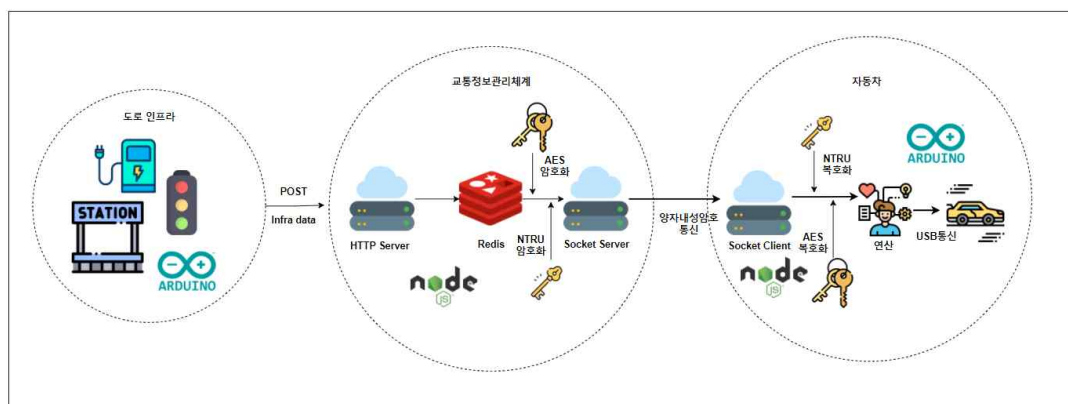


- 안전성이 가장 뛰어난 양자 내성 암호 NTRU 알고리즘 방식을 적용한, 차세대 하이브리드 암호화 교통정보체계(V2X) 보안 모바일 망 서비스 구현

#### 2) H/W 구성도



#### 3) S/W 구성도



## 2. 작품 기능

### 1) 전체 기능 목록

#### (1) 교통정보체계

구분	기능	설명	현재진척도(%)
S/W	인프라 데이터 수집	HTTP POST 통신을 통해 인프라 데이터를 수집한다.	100
	인프라 데이터 저장	redis를 이용하여 인프라 데이터를 임시 저장한다.	100
	키 생성 및 교환	양자 내성 NTRU 알고리즘을 사용한 암호화 통신을 위해 NTRU 공개키를 주고받는다.	100
	메시지 암호화 및 전송	난수의 AES 대칭키를 통해 메시지를 암호화하고 수신자의 NTRU 공개키를 통해 AES 대칭키를 암호화 후 암호문을 합쳐 전송한다.	100
	유저 인터페이스	웹 소켓 통신 활성화 및 키 교환, 암호화 과정을 웹 뷰 형태로 제공해준다.	100

#### (2) 자동차(통신모듈)

구분	기능	설명	현재진척도(%)
S/W	키 생성 및 교환	양자 내성 NTRU 알고리즘을 사용한 암호화 통신을 위해 공개키를 주고받는다.	100
	암호문 복호화	암호문을 분해 후 AES 대칭키는 NTRU 개인키로, 메시지는 복호화된 AES 대칭키로 복호화하여 메시지를 얻는다.	100
	유저 인터페이스	웹 소켓 통신 활성화 및 키교환, 복호화 과정을 웹 뷰 형태로 제공해준다.	100
	시리얼 통신	USB 시리얼 통신을 통해 자동차 아두이노에게 움직임 신호를 전달한다.	100

#### (3) 자동차(기능)

구분	기능	설명	현재진척도(%)
S/W	시리얼 통신	자동차 통신 모듈에게 받은 신호에 따라 모터쉴드를 동작하여 이동 또는 정지한다.	100
H/W	라인 트레이싱	적외선 IR 센서를 통해 검은색 라인을 측정한다.	100
	모터 동작	모터쉴드를 사용하여 자동차가 움직일 수 있도록 모터를 제어한다.	100

(4) 인프라(신호등)

구분	기능	설명	현재진척도(%)
S/W	인프라 데이터 처리	신호등 색깔이 바뀌면 교통정보관리체 계로 신호등 데이터를 전달한다.	100
H/W	신호등 모듈 LED 점등	신호등 모듈을 이용해 LED를 점등한다.	100

(5) 인프라(위치 정보)

구분	기능	설명	현재진척도(%)
S/W	위치 정보 데이터 처리 및 전송	ESP-01모듈을 사용하여 자동차의 위치 정보를 알려준다.	100
H/W	조도 센서 값 수집	기준 미만의 조도 센서값을 파악하여 자동차 현재 위치를 수집한다.	100

(6) 인프라(정류장)

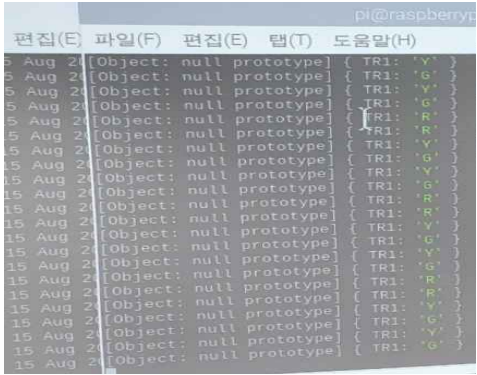
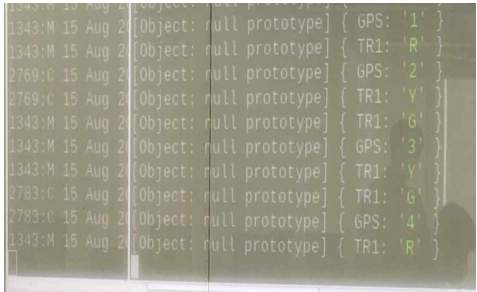
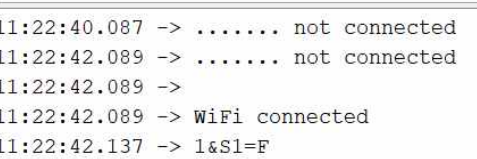
구분	기능	설명	현재진척도(%)
S/W	승객 정보 데이터 처리 및 전송	정류장 승객 유무를 교통정보체계로 넘겨준다.	100
H/W	승객의 유무 확인	적외선 센서를 이용하여 승객의 유무 를 확인한다.	100

2) S/W 주요 기능

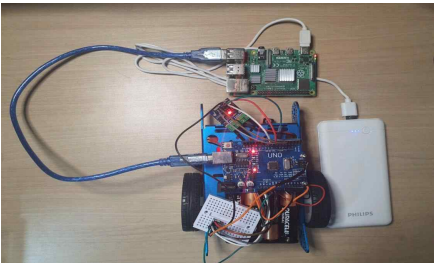
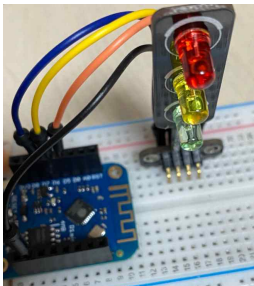
기능	설명	작품실물사진
인프라 데이터 처리	HTTP POST 통신을 통해 인프라 데이 터를 수집한다. Redis를 통해 인프라 의 상태를 임시 저장한다.	<pre> 127.0.0.1:6379&gt; keys * 1) "S2" 2) "TR1" 3) "GPS" 4) "TR2" 5) "S1" 127.0.0.1:6379&gt; mget S1 S2 TR1 TR2 GPS 1) "F" 2) "F" 3) "R" 4) "G" 5) "10" 127.0.0.1:6379&gt; </pre>
키 생성 및 교환 (교통정보체계)	양자 내성 알고리즘이 적용된 하이브 리드 암호화 시스템을 구축하기 위한 공개키, 개인키 생성 및 교환한다.	


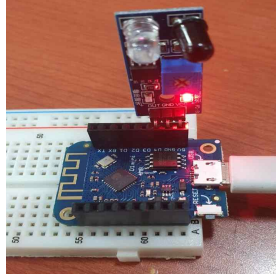
기능	설명	작품실물사진
메시지 암호화 및 전송(교통정보체계)	Redis에서 가져온 인프라 데이터를 JSON 형식으로 정형화 한 후 암호화 하여 암호문을 전송한다. 랜덤 생성한 AES 대칭키로 데이터를 암호화하고 수신자의 NTRU 공개키로 대칭키를 암호화 후 암호문을 만들어 전송한다.	
키 생성 및 교환(자동차 통신모듈)	양자 내성 알고리즘이 적용된 하이브리드 암호화 시스템을 구축을 위한 공개키, 개인키 생성과 교환을 한다.	
암호문 복호화(자동차 통신모듈)	암호문을 암호화된 대칭키와 메시지로 분해 후 대칭키는 NTRU 개인키로, 메시지는 복호화된 AES대칭키로 복호화하여 메시지를 얻는다.	
유저인터페이스	웹 소켓 통신 활성화 및 키교환, 암호화 과정을 웹 뷰 형태로 제공해준다.	
자동차 line-tracing	자동차 라즈베리파이와의 시리얼 통신으로 입력된 문자에 따라 자동차의 동작이 결정된다. 입력된 문자가 'T'이면 직진하고 'F'이면 정지한다.	



기능	설명	작품실물사진
신호등 인프라 데이터 처리	Wemos D1을 웹 서버와 연동하여 통신할 수 있고, 신호등 모듈 인프라로부터 측정값을 받아와 교통정보체계에 데이터를 넘겨준다.	
위치정보 데이터 처리 및 전송	조도 센서의 값을 읽어 자동차의 위치정보를 알려준다.	
승객 정보 데이터 처리 및 전송	적외선 센서를 이용하여 승객의 유무를 확인한다.	

### 3) H/W 주요 기능

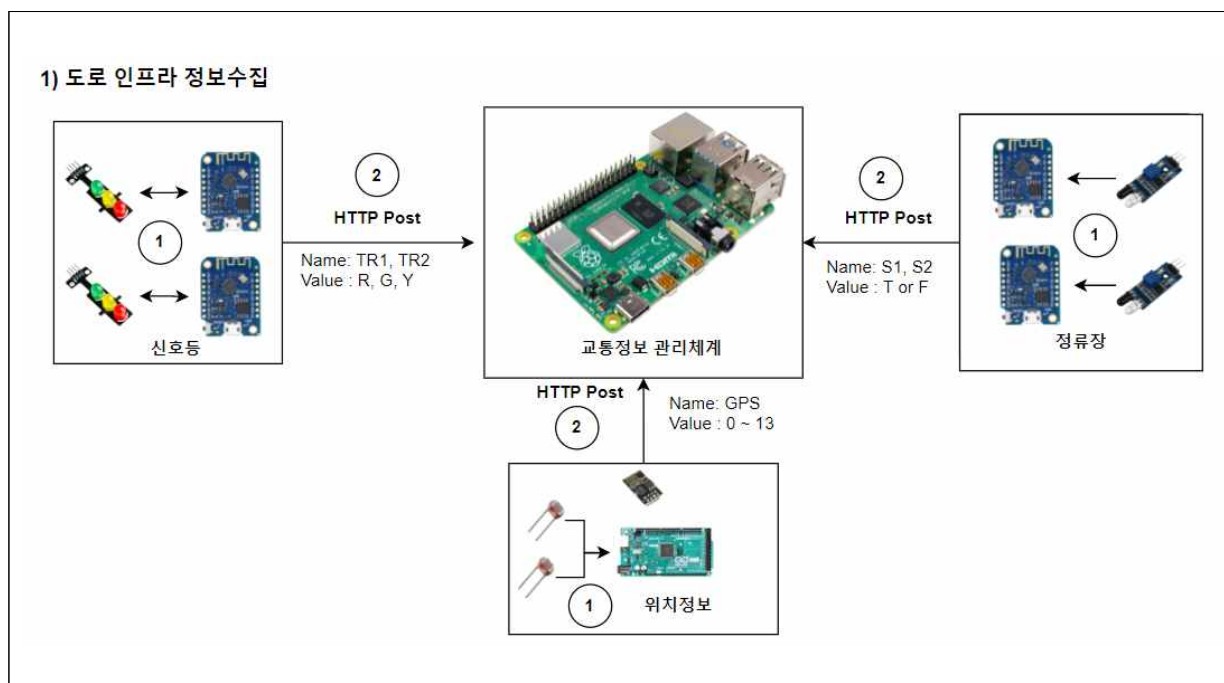
기능/부품	설명	작품실물사진
자동차 시리얼 통신	자동차 통신모듈(라즈베리파이)와 아두이노가 USB 시리얼 통신으로 연결된다.	
신호등 LED 모듈	신호등 모듈의 LED 점등으로 설정한 시간 차에 따라 신호 표시를 알려준다.	

기능/부품	설명	작품실물사진
조도 센서 (GPS)	ESP-01모듈을 사용하여 웹 서버에 접속하고, 기준 미만의 조도 센서값을 파악하여 교통정보체계로 위치정보 데이터를 넘겨준다.	
정류장 적외선 센서	적외선 센서를 이용하여 승객의 유무를 확인한다.	

### 3. 주요 적용 기술

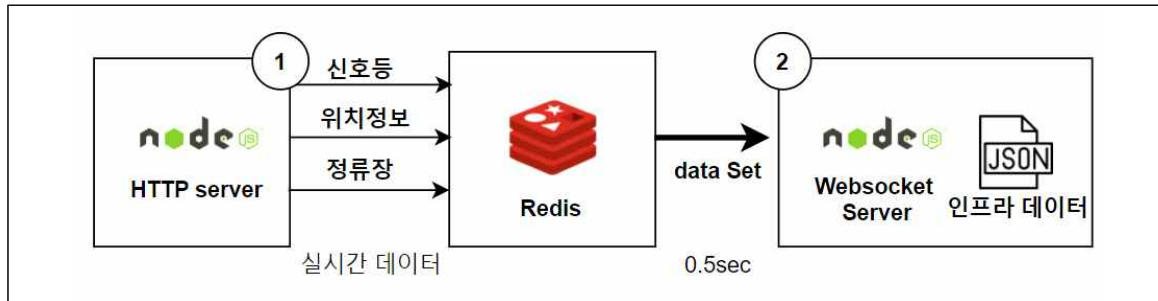
#### 1) 도로 인프라 정보수집 : 센서 정보수집, HTTP POST

- ① Wemos D1과 아두이노 메가를 통해 인프라 센서값을 수집한다.
- ② 인프라 상태가 바뀔 때마다 HTTP POST 통신을 통해 센서값을 교통정보관리체계로 전송한다.



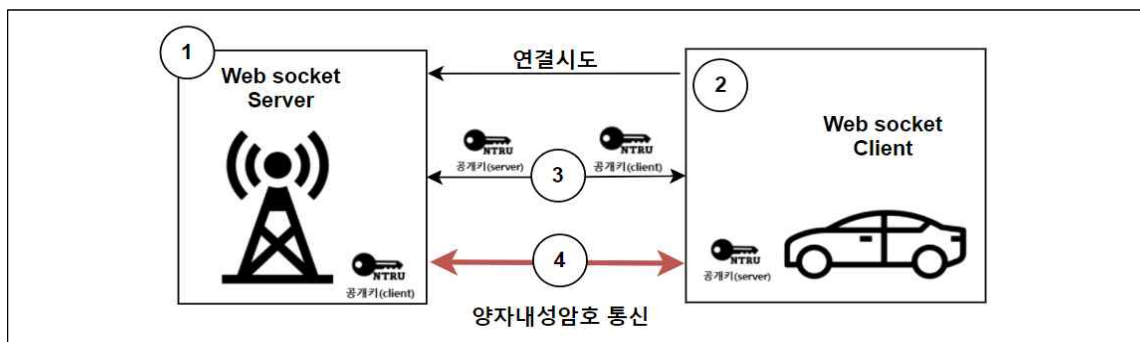
## 2) 인프라 정보 저장 및 병합 : Redis

- ① 교통정보관리체계는 인프라 데이터를 받아 데이터베이스 관리 시스템인 redis에 저장한다.
- ② 0.5초마다 reids의 인프라 데이터를 모두 불러와 JSON 형식으로 병합한다.



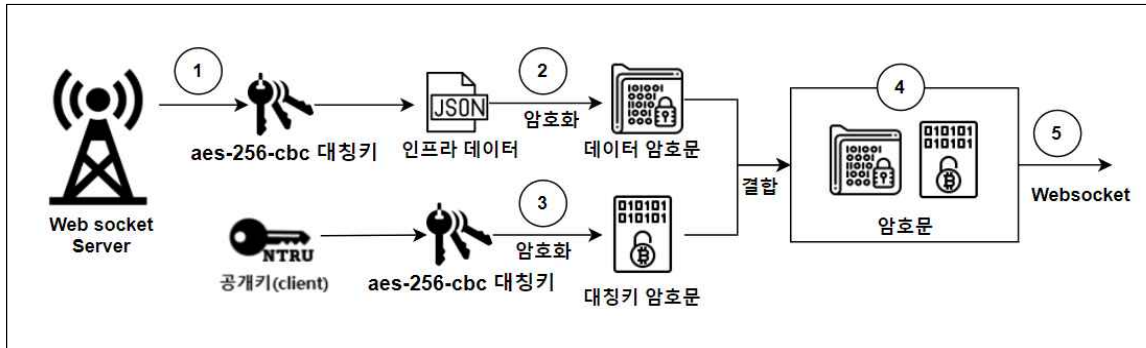
## 3) 양자 내성 암호 연결 설정 관계 수립

- ① 교통정보관리체계가 Node.js를 통해 웹 소켓 서버를 활성화한다.
- ② 자동차 Node.js를 통해 활성화한 웹 소켓 연결을 시도한다.
- ③ 연결되면 NTRU 알고리즘을 통해 암호화하는 시스템인지 확인하기 위해 공개키를 교환한다.
- ④ 공개키 교환을 마치면 연결 관계가 수립된다.



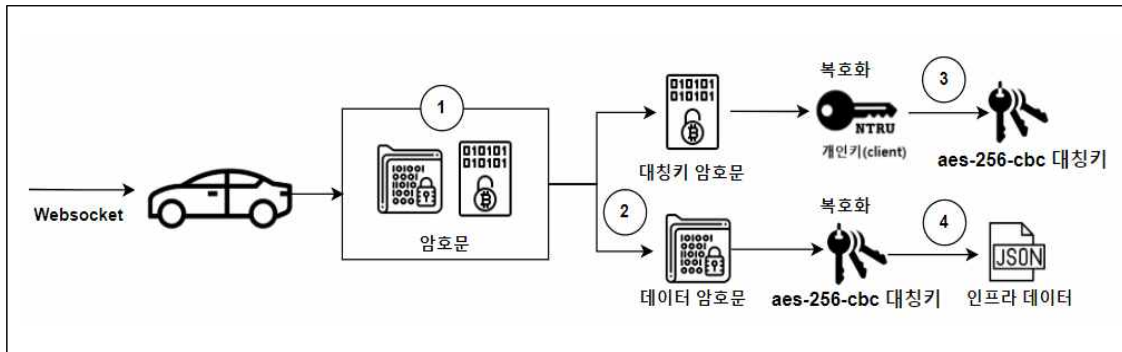
## 4) 인프라 정보 암호화 및 송신

- ① 난수 생성기를 통해 20byte의 난수를 생성하고 이를 aes-256-cbc로 암호화 대칭키로 사용한다.
- ② 대칭키를 사용하여 JSON 형태로 병합된 인프라 정보를 aes-256-cbc로 암호화한다.
- ③ 수신자의 NTRU 공개키를 사용하여 인프라 정보 암호화에 사용된 대칭키를 양자 내성 암호화한다.
- ④ 대칭키로 암호화된 인프라 정보와 공개키로 암호화된 대칭키를 병합하여 암호문을 만든다.
- ⑤ 웹 소켓을 통해 교통정보체계는 자동차에게 암호문을 전송한다.



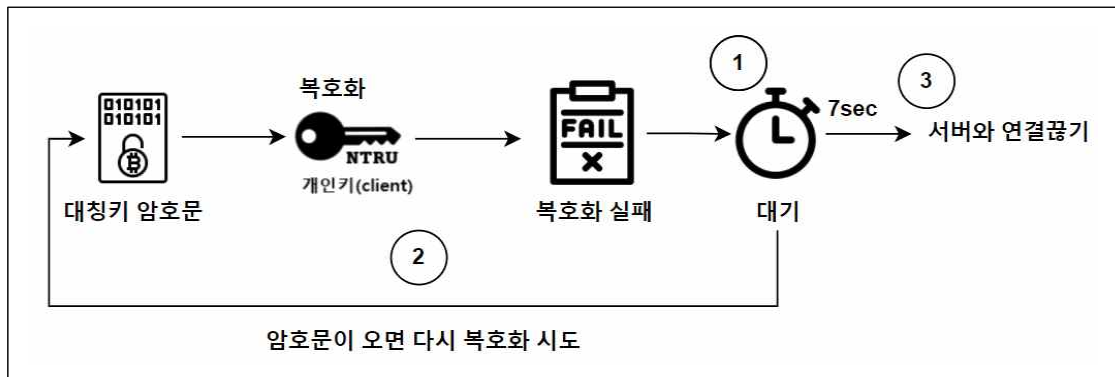
## 5) 인프라 정보 수신 및 복호화 성공

- ① 웹 소켓을 통해 암호문을 수신한다.
- ② 암호화된 인프라 정보와 대칭키를 분해한다.
- ③ 자동차의 NTRU 개인키를 통해 NTRU 암호화된 aes-256-cbc 대칭키를 복호화한다.
- ④ 복호화된 aes-256-cbc 대칭키를 통해 암호화된 인프라 정보를 복호화한다.



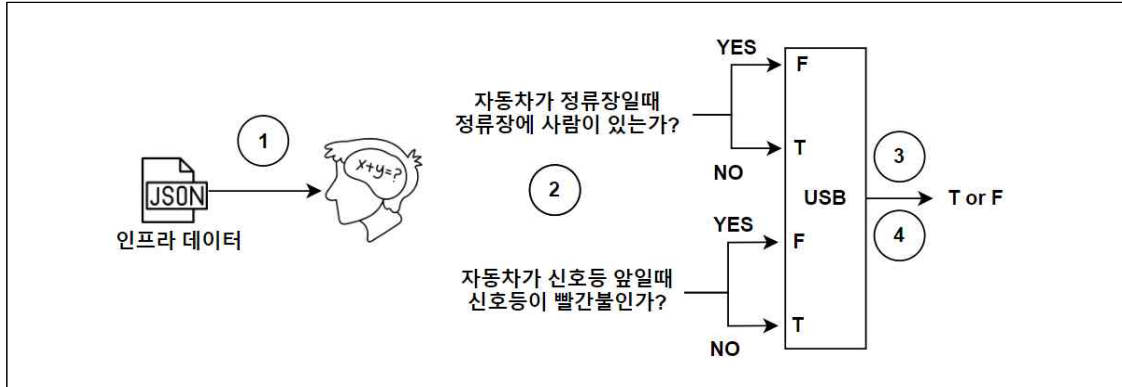
## 6) 인프라 정보 수신 및 복호화 실패

- ① 복호화 실패 시 타이머를 두어 암호문이 오길 기다린다.
- ② 암호문이 오면 다시 복호화를 시도한다.
- ③ 일정 시간 암호문이 오지 않으면 잘못된 연결임을 판단하고 서버와 연결을 끊는다.



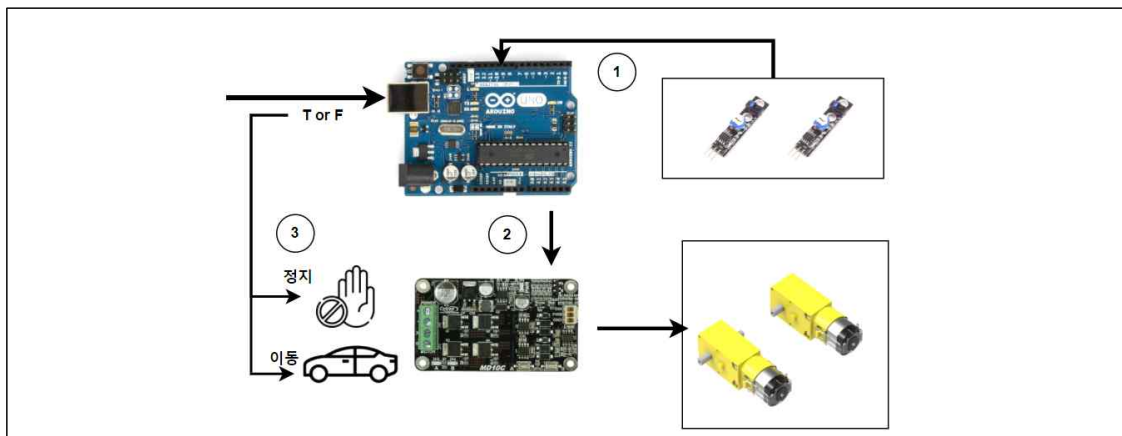
## 7) 정보 가공 및 신호 전달

- ① JSON 형태로 복호화한 인프라 정보를 확인한다.
- ② 위치정보 인프라의 값을 바탕으로 다른 인프라의 상태를 비교한다.
- ③ 자동차가 멈춰야 할 상황이면 'F' 를 USB 통신을 통해 전송한다.
- ④ 자동차가 이동해야 할 상황이면 'T' 를 USB 통신을 통해 전송한다.



## 8) 안전한 자율 주행 모드

- ① 적외선 IR 송수신 센서를 통해 자동차가 지나가야 할 검은 라인을 확인한다.
- ② 모터 쉴드를 제어하여 통해 자동차를 움직인다.
- ③ USB 통신을 통해 받은 값에 따라 모터를 작동시켜 인프라 정보에 따라 자동차가 움직인다.



#### 4. 작품 개발 환경

구분		상세내용
S/W 개발환경	OS	window, raspbian
	개발환경(IDE)	Arduino IDE, VIM
	개발도구	라즈베리파이, PC
	개발언어	웹 프론트(ejs, css, jquery), 웹 백엔드(node.js)
	기타사항	reids, websocket
H/W 구성장비	디바이스	Wemos D1, 아두이노 메가
	센서	조도 센서, 적외선 송수신 센서, 근접 센서
	통신	HTTP(POST), WEB socket(양자 내성 암호 통신)
	언어	C++, Node.js
	기타사항	인프라 신호등(신호등 모듈), 자동차 동작부(라인트레이서 자동차)
프로젝트 관리환경	형상관리	집 보관
	의사소통관리	NOTION
	기타사항	NOTION, gitlab

#### 5. 기타 사항 [본문에서 표현되지 못한 작품의 가치(Value)] 및 제작 노력

##### - 여러 양자 내성 암호 중 NTRU를 선택한 이유와 그 강점

Peter Shor에 의해 소인수분해 문제를 다항식 시간으로 해독할 수 있는 알고리즘이 소개된 후 RSA 암호화 체계를 사용하는 모든 서비스가 큰 보안 위협에 처하게 된다. 또한, 양자컴퓨터 개발의 가속으로 새로운 암호 알고리즘의 필요성이 제기되었다.

미국 표준 기술 연구소 NIST에서는 양자 내성 암호의 표준화된 알고리즘을 선정하기 위해 콘테스트를 통해 안정성을 비교하고 있다. 3라운드에 거쳐 평가가 이루어졌는데, 2020년 Classic McEliece, CRYSTALS KYBER, NTRU, SABER, CRYSTALS DILITHIUM, FALCON, Rainbow 7개의 알고리즘과 8개의 후보군이 선정되었다. 이는 2021년까지 검증이 이루어질 예정이다. 따라서 위 7개의 알고리즘은 이미 두 차례에 걸쳐 검증이 진행된 것으로, 아직 표준화되지는 않았지만, 프로젝트를 진행하는 입장에서 양자 내성 암호의 역할을 할 수 있을 것으로 판단했다.

[표 2] NIST PQC 3라운드 진출 알고리즘 분류

	3라운드		대안 알고리즘	
	알고리즘	분류	알고리즘	분류
PKE/ KEM	Classic McEliece	부호기반암호	BIKE	부호기반암호
	CRYSTALS KYBER	LWE	FrodoKEM	LWE
	NTRU	NTRU	HQC	부호기반암호
	SABER	LWR	NTRU Prime	NTRU
			SIKE	Isogeny
전자서명	CRYSTALS DILITHIUM	LWE	GeMMS	MQ
	FALCON	NTRU	Picnic	대칭키암호
	Rainbow	다변수	Sphincs+	Hash

(자료) 조선대학교 자체 작성

<양자 내성 암호 표준화 모델>

이번 프로젝트의 목표는 양자 내성 암호를 통해 자율 주행 자동차와 차세대 교통정보체계가 안전하게 연동될 수 있도록 하는 것이다. 따라서 안전하게 데이터를 보내는 것이 목표이므로 데이터를 암호화하는 대칭키가 탈취되는 것을 막아야 해서 양자 내성 암호의 2가지 방식(키 암호화 방식, 디지털 서명 방식) 중 하나인 키 암호화 방식을 선택했다.

PKE/KEM 알고리즘 중 NTRU를 선택한 이유는 다른 알고리즘과 비교했을 때 높은 안정성을 가지기 때문이다. NTRU는 1996년 처음 제안된 이후로 25년이 지난 지금까지 많은 공격 시도에도 불구하고 유효한 공격이 알려지지 않았다. 그만큼 공격에 대해서 저항한다는 것이고, 이에 따라 신뢰를 받는 알고리즘이다. 또한, RLWE와 MLWE와 같은 알고리즘들과는 전혀 다른 문제에 기반을 두고 있어서 다양성을 통해 표준화의 안전성에 기여할 수 있다.

기존의 RSA와 비교한 암호 강도를 비교한 표를 보면, 단위시간에 RSA는 500,000개의 키값을 비교하지만, NTRU는 180,000개의 키를 비교한다. key generation speed로 단순 비교해봤을 때 NTRU는 RSA보다 약 3배 정도 복호화에 많은 시간이 소요된다. 따라서 NTRU는 RSA에 높은 보안 강도를 가지고 있어 이에 대한 대체제가 될 수 있을 것으로 보인다.

Table 1: Comparison of public key algorithms

Algorithm	Keys length (bits)	Key generation speed	Encryption speed	Decryption speed
RSA	1024	500,000	9090	781
ECDSA	163	1424	1424	2183
NTRU <sub>sign</sub>	251	180,000	500	303

#### 〈NTRU-RSA 보안 강도 비교〉



### III. 프로젝트 수행 내용

※ 평가항목 : 수행능력 (문제해결능력, 수행충실성)

#### 1. 프로젝트 수행일정

프로젝트 기간 (ICT멘토링 사이트 기준)		2021.03.30. ~ 2021.11.30.									
구분	추진내용	프로젝트 기간									
		3월	4월	5월	6월	7월	8월	9월	10월	11월	12월
계획	프로젝트 내용 이해와 구체적인 구현 아이디어 제시										
분석	개발에 필요한 핵심 기능 분석										
설계	시스템 흐름도 작성										
	센서 하드웨어 설계 및 기능 구현										
개발	물품 준비										
	프로토 타입 제품 제작										
	실제 작품 제작										
테스트	올바르게 작동하는지 테스트 및 보완										
종료	결과보고서 제출										

#### 2. 프로젝트 추진 과정에서의 문제점 및 해결방안

##### 1) 작품 개발 측면

##### - 교통정보체계와 자동차 사이의 양자 내성 암호 통신 구현

교통정보체계와 자율주행자동차 간 안전한 통신을 위해 양자 내성 암호 통신 방법을 알아보던 도중 Openquantumsafe 라는 프로젝트 사이트를 알게 됐다. Openquantumsafe에서는 TLS/SSL 기반 Applications and protocols를 Docker형태로 제공해줬고, 우리 팀은 현재 많이 사용되는 HTTPS를 사용한 서비스 제공을 목표로 자료 조사를 하였다. 하지만 우리 프로젝트에서 Client는 자동차로 Openquantumsafe에서 제공하는 HTTPS client인 Curl나 Chromium을 사용한 환경 구축이 어려웠다. 이를 해결하기 위해 자체적인 Client 환경을 만들기 위해 노력했지만, Openquantumsafe에서 제공하는 Server와 약속된 환경을 Client인 라즈베리파이에 구축하는 방법을 찾지 못했다. 하지만 이 과정을 통해 Server와 Client간의 약속을 통해 양자 내성 암호 통신이 가능하다는 것을 알게 됐고, 우리 팀은 웹 소켓을 통한 자체적인 프로토콜을 만드는 방향으로 서비스 제공 방향을 선택할 수 있었다. Node.js에서 제공하는 NTRU 알고리즘을 바탕으로 공개키, 개인키를 생성하여 공개키를 교환하는 과정을 통해 연결 관계를 수립하였고, 상대방의 공개키를 난수 생성된 대칭키를 암호화하는 방법으로 안전한 데이터 전송을 보장할 수 있었다.



### - 라인트레이서 자동차 동작 기능 구현

자동차 라즈베리파이로부터 오는 USB 전원만으로 자동차의 전원을 공급하려고 하였지만, 전압이 부족해 자동차가 제대로 동작하지 못하는 것을 확인하였다. 이를 해결하기 위해 모터 드라이브와 아두이노 전원을 따로 공급하는 방안을 생각했다. 하지만 모터 드라이브 L923D에서 어떤 핀을 연결해야 아두이노와 전원은 공유하지 않지만, 그 기능을 다 할 수 있을지를 파악하지 못했고 이에 많은 시간이 소요되었다. 그 후, L9110S에서 Motor A, B, GND와 VCC만을 연결하여 모터 쉘드를 동작시키는 다는 것을 알게 되었고, L923D에도 같은 방법으로 할 수 있을 것으로 생각했다. 하지만 아두이노와 모터 드라이브 L923D의 전원을 분리하려는 시도에서 모터 드라이브의 5V전원 핀을 끊어버렸고 현재 가지고 있는 모터 드라이브 L923D로는 동작을 구현할 수 없다는 것을 알게 되었다. 코딩을 전체적으로 수정해야 해서 주저했었지만 보유한 L923D로는 할 수 없었기 때문에 원래 가지고 있던 L9110S으로 대체하기로 결정하였다. 최종적으로 L9110S는 6V 건전지로, 아두이노는 라즈베리파이의 USB 전원으로 전원을 공급하여 라인트레이싱이 동작할 수 있도록 하였다.

모터 드라이브 L9110S를 사용했을 때 라인을 따라가지 못하고 직진만 우선적으로 동작하는 상황이 발생했다. 시리얼 모니터로 하나하나 살펴보면서 원인이 무엇인지 파악하려고 하였고, 자동차가 처음에 라인 위에 있는 상황에서의 동작만 일어나고 라인의 변화에 따른 반응이 없다는 것을 인지했다. 처음에 입력되는 라인 트레이싱 모듈의 반응과 상관없이 라인의 변화에 따라 직진, 우회전, 좌회전의 기능이 동작하도록 while문으로 코딩을 수정하였고 line-tracing 이 정상적으로 동작하는 것을 확인할 수 있었다.

### - 인프라(신호등, 정류장, GPS 등)와 교통정보체계 사이의 데이터 전송

각 모듈의 값을 교통정보체계(서버)로 데이터 전송하는 과정에서 조금 어려움을 겪었다. 그 이유는, 코로나19로 인해 오프라인 미팅을 최소화하는 과정에서 팀원들끼리 자주 모일 수 없었고, 각각의 모듈의 값은 서버나 라즈베리파이를 동작시킬 경우에서만 데이터값을 전송할 수 있었다. 이에 대한 해결책으로 zoom을 이용한 온라인 미팅을 하면서 팀 내 상호작용하여 실시간으로 서버를 작동시켜, 원하는 데이터 값을 주고받을 수 있게 되었다.

## IV. 작품의 기대효과 및 활용분야

### ※ 평가항목 : 기획력 (활용가능성)

#### 1. 작품의 기대효과

- C-ITS(협력 기능형 교통 체계)를 구축하기 위한 기본 토대가 된다.

C-ITS는 인프라-차량(V2I), 차량-차량(V2V)이 유무선으로 정보를 주고받아 보행자나 차량 위치 데이터 등을 공유하여 실시간 주행에 활용하고, 전체 차량이 수집한 교통 상황을 종합해 교통 체증을 분산하는 고도화된 체계를 말한다. 만약 이러한 자율 자동화 기반 차세대 교통 체계가 양자컴퓨터가 도입되면서 해커에 의해 좌우된다면 큰 혼란이 발생할 것이다. 따라서 이에 따라 높은 강도의 보안 수준이 요구된다. 양자 내성 알고리즘을 통해 구현된 암호문으로 네트워크 안정성을 극대화해 신뢰성 있는 서비스 구현을 위해 필요한 기반을 다질 수 있다.

- 운전자나 차량 탑승자의 안전을 보장할 수 있다.

최근 자동차가 자율 주행으로 바뀌는 움직임이 계속되고 있는데 보안이 허물어져 해커가 자동차를 제어할 수 있다면 차량 탑승자의 안전이 위협해진다. 새로운 보안 체계를 통해 자율 주행 자동차를 믿고 이용할 수 있도록 인식시켜야 한다. 보안이 없는 서비스는 오히려 독으로 다가올 수 있어 이 점에 주의할 필요가 있다.

- NTRU 알고리즘에 관한 심화 연구에 도움이 된다.

NTRU 알고리즘만을 해결하기 위한 tool이 아직 없는 현실점에서 앞으로 그에 대한 tool이 생긴다면 그것이 효과적인지 확인할 수 있는 좋은 모델이 될 것이다.

- 새로운 암호 보안이 실제 교통 환경에서 적용될 가능성을 확인한다.

프로젝트 규모와 예산으로 인해 실제 자동차로 진행할 수는 없었지만, 신호등, 정류장, 주유소 등의 인프라를 추가하여 최대한 비슷한 환경을 만들고자 하였다. 간소화한 모델에서 보안이 잘 작동하기 때문에 이를 실제 자동차에 적용하여 진행할 수 있는 수준이라고 볼 수 있다. 따라서 이번 프로젝트를 통해 구현한 보안 수준은 실제 교통 환경에서도 적용할 수 있는 것으로 보인다.

- 다음 양자 내성 암호 기반 교통관리체계의 선행연구가 된다.

이번 프로젝트에서 격자 기반의 NTRU 알고리즘을 이용하여 암호화했던 것처럼 현재 구축된 교통관리체계에서도 관련 요구가 많은 상황이다. 양자컴퓨터로 인한 기존 암호체계의 붕괴가 예견된 시점에서 이를 적용한 교통관리체계 모델은 없는 것으로 보인다. NTRU 양자 내성 알고리즘을 적용한 교통 시스템은 이를 위한 선행연구이자 다음 단계로 가는 과정이 된다. 다른 알고리즘으로 관리체계를 만들려고 할 때 이번 결과물이 도움이 될 것으로 예상된다.

## 2. 작품의 활용분야

### - 양자 컴퓨팅 해킹 예방

양자 컴퓨팅 기술의 급격한 발전은 기존 암호화 기술에 대한 손쉬운 해킹이 가능할 것이라는 우려가 현실이 되어 실질적 보안 위협으로 인식되고 있다. 이에 양자 내성 암호 통신을 하면 양자컴퓨터로 인한 해킹 위협에서 벗어날 수 있다. 특히 국방, 금융, 의료 산업 등, 강력한 보안이 있어야 하는 분야에서 양자 내성 암호 통신을 통해 보다 안전한 통신이 가능하다.

### - 안전한 V2X 통신 지원

교통 환경이 점점 자율 주행, 지능형 교통 시스템으로 발전하면서 차량과 차량 및 인프라와 연결성이 확대되고 있으며 복잡한 소프트웨어 및 외부 연결성을 가지는 자동차는 다양한 보안 위협에 노출되어 있다. 이에 보다 안전한 통신이 수반되어야 하는데, 양자 내성 암호 통신을 통해 해킹으로 인한 자율 주행 사고, 오작동을 최소화하여 안전한 도로 주행이 가능하게 한다.