presentation

IoT와 BLE 통신에서 형태보존암호를 활용한 데이터 암호화 통신

소속 : 한성대학교
이름 : 임지환, 김도영

CONTENTS

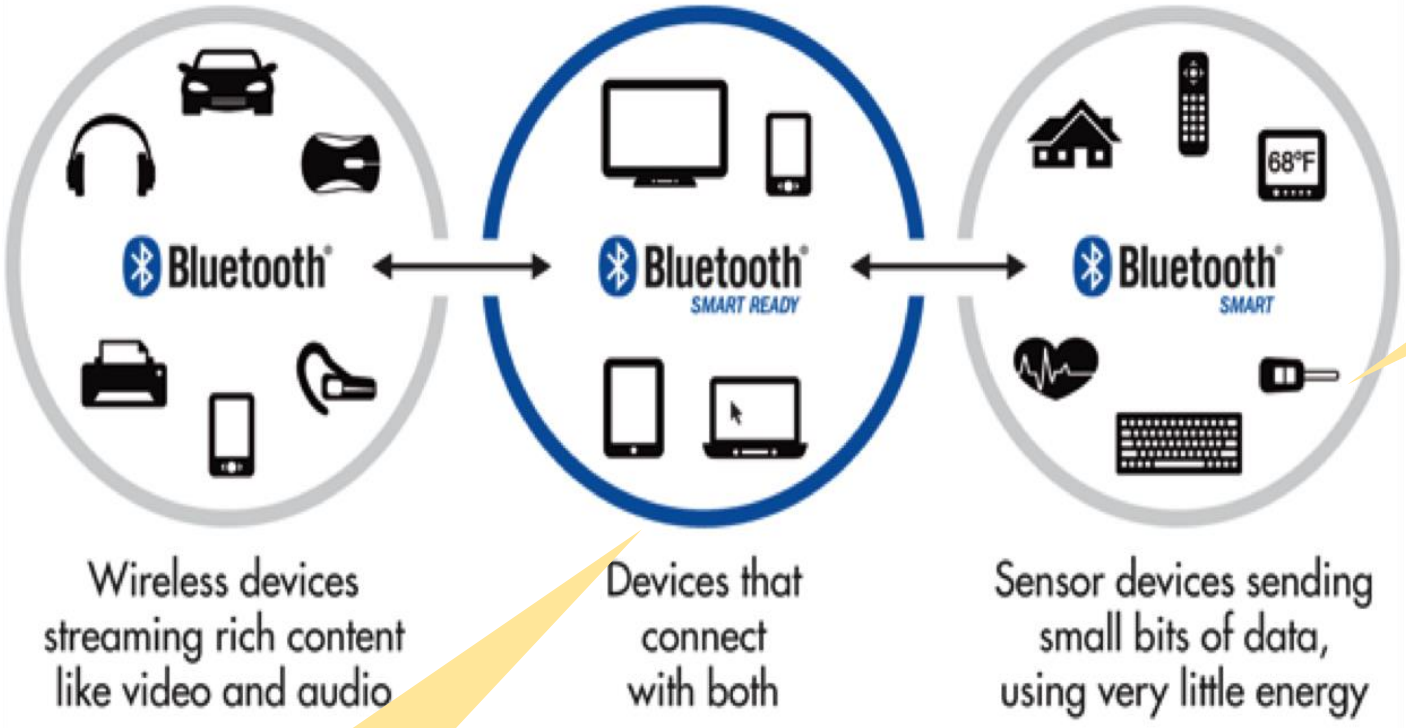
presentation

1. Bluetooth Low Energy (BLE)

01 | What is BLE?

IoT와 BLE 통신에서 형태보존암호를 활용한 데이터 암호화 통신

기존의 Bluetooth Classic 보다 훨씬 적은 전력을 사용하여 Classic과 비슷한 수준의 무선 통신



Ex) IoT Sensor

Ex) Smart Phone

각 구간에 Data 암호화 필요

01 | How they communicate?

BLE를 지원하는 디바이스들은 기본적으로 Advertise(Broadcast) 와 Connection 이라는 방법으로 외부와 통신한다.

1.Advertise mode(1대 다 통신)

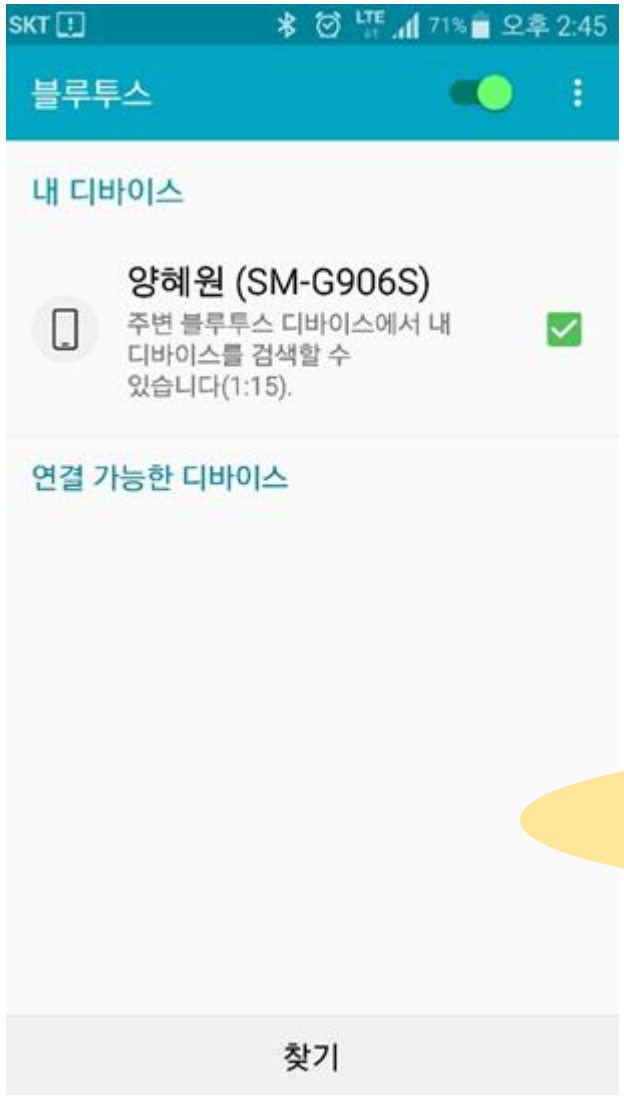
- 작은 데이터(31b 이하)나 신호를 보낼 때, 1대 다 통신으로 'advertise'는 말 그대로 신호를 뿌리는 것이기 때문에 보안성이 매우 취약하다. 따라서 advertise mode에서 data를 암호화 했을 때, 효과를 크게 볼 수 있는 것

2.Connection mode(1대 1통신)

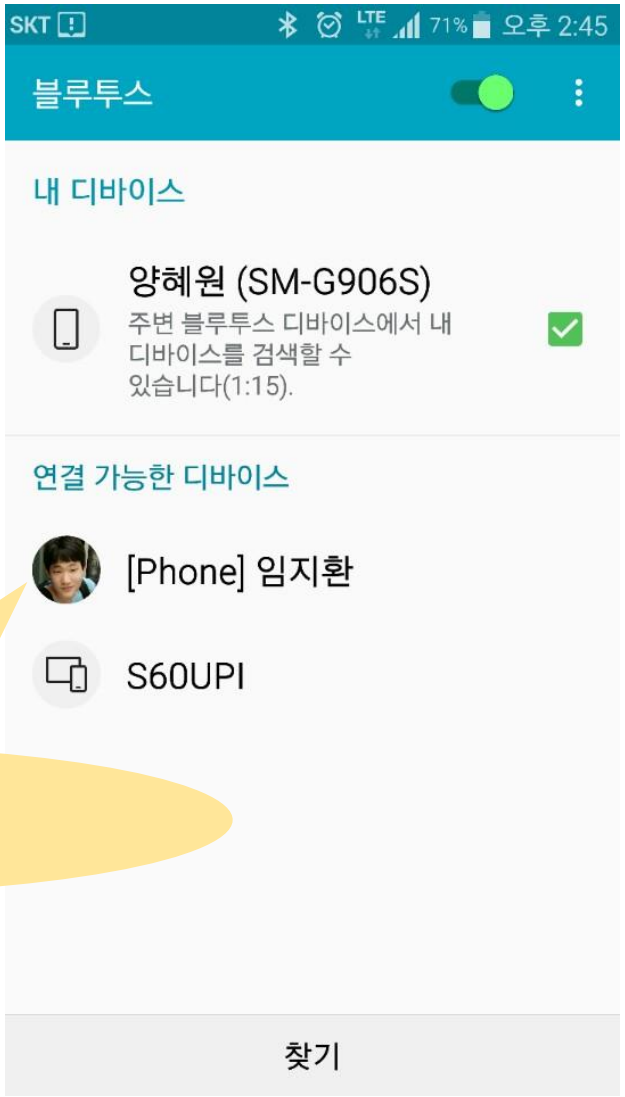
- 양방향으로 데이터를 주고받거나, Advertising Packet으로만 전달하기에는 많은 양의 데이터를 주고 받아야 하는 경우에는, Connection Mode로 통신을 한다. Advertise처럼 '일대다' 방식이 아닌, '일대일' 방식으로 디바이스 간에 데이터 교환이 일어난다. 디바이스간에 Channel hopping 규칙을 정해놓고 통신

01 | Advertise mode(1대 다 통신) (2) (예시)

IoT와 BLE 통신에서 형태보존암호를 활용한 데이터 암호화 통신

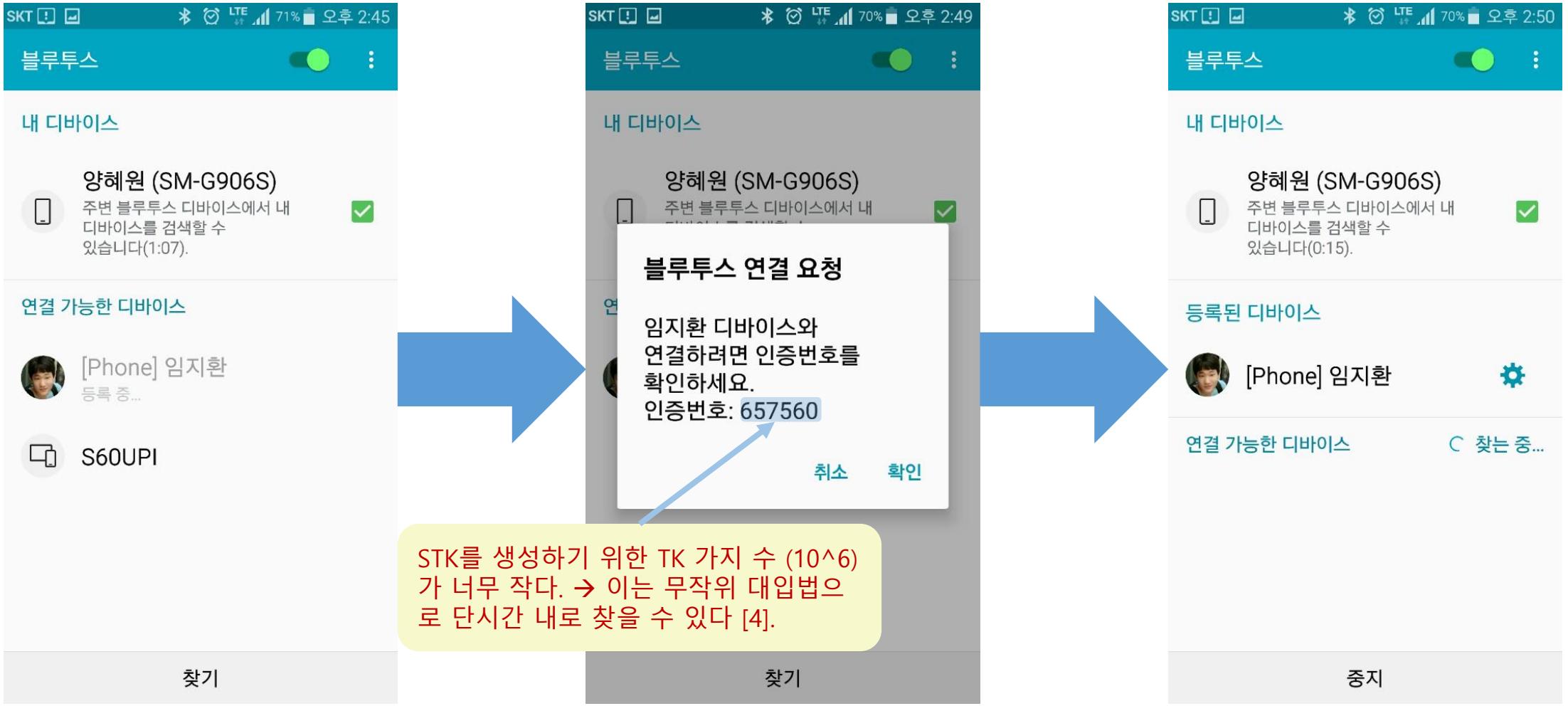


1. Advertising Paket 전송
2. Scan REQ
3. Scan RSP



01 | Connection mode(1대 1통신) (2) (예시)

IoT와 BLE 통신에서 형태보존암호를 활용한 데이터 암호화 통신



presentation

2. Related Works

02 | Related Works

IoT와 BLE 통신에서 형태보존암호를 활용한 데이터 암호화 통신

BLE 관련 연구

2016 년 에 Bluetooth Special Interest Group (SIG)는 6년 만에 블루투스 5.0을 선보여 기존 Bluetooth 4.0보다 통신거리 4배, 통신속도 2배, Pairing 문제 해결 등등 기존보다 진보된 무선통신 기술을 내놓았다 [1].

BLE 보안의 취약점으로 연결하는 과정 중 하나인 Pairing에서 STK를 생성하기 위해 사용되는 TK의 가짓수가 너무 적다는 것이다 [2].

.

블루투스 기반 비콘은 현재 여러 IT산업에서 활발히 적용됨에 따라 관련 보안 방법들이 제안되고 있지만, 아직 활용 분야별 세부적인 해커의 공격에 대한 대응 방안과 보안 모듈 개발에 대해서는 추가적인 연구가 필요한 상황이다 [3].

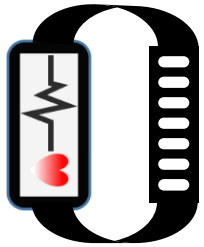
IoT 대상 기기의 경우 처리속도 및 저장소 제약 문제로 인해 암호화를 적용하기 힘든 경우가 많이 존재한다 [6].

presentation

3. Proposal Method

03 | Proposal Method

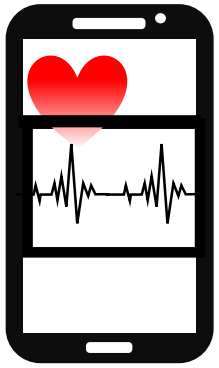
IoT와 BLE 통신에서 형태보존암호를 활용한 데이터 암호화 통신



스마트 밴드

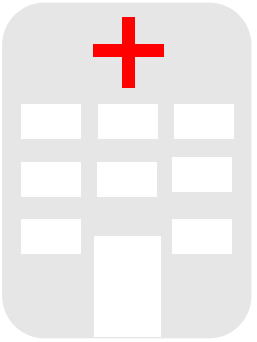
1. 의료기기와 스마트폰을
연동하여 환자의 정보 측정

블루투스 연결

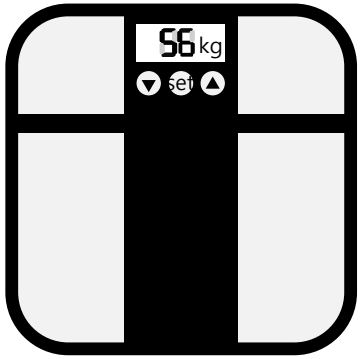


스마트폰

2. 평문으로 된 환
자의 데이터를 전송



병원



체성분 분석기

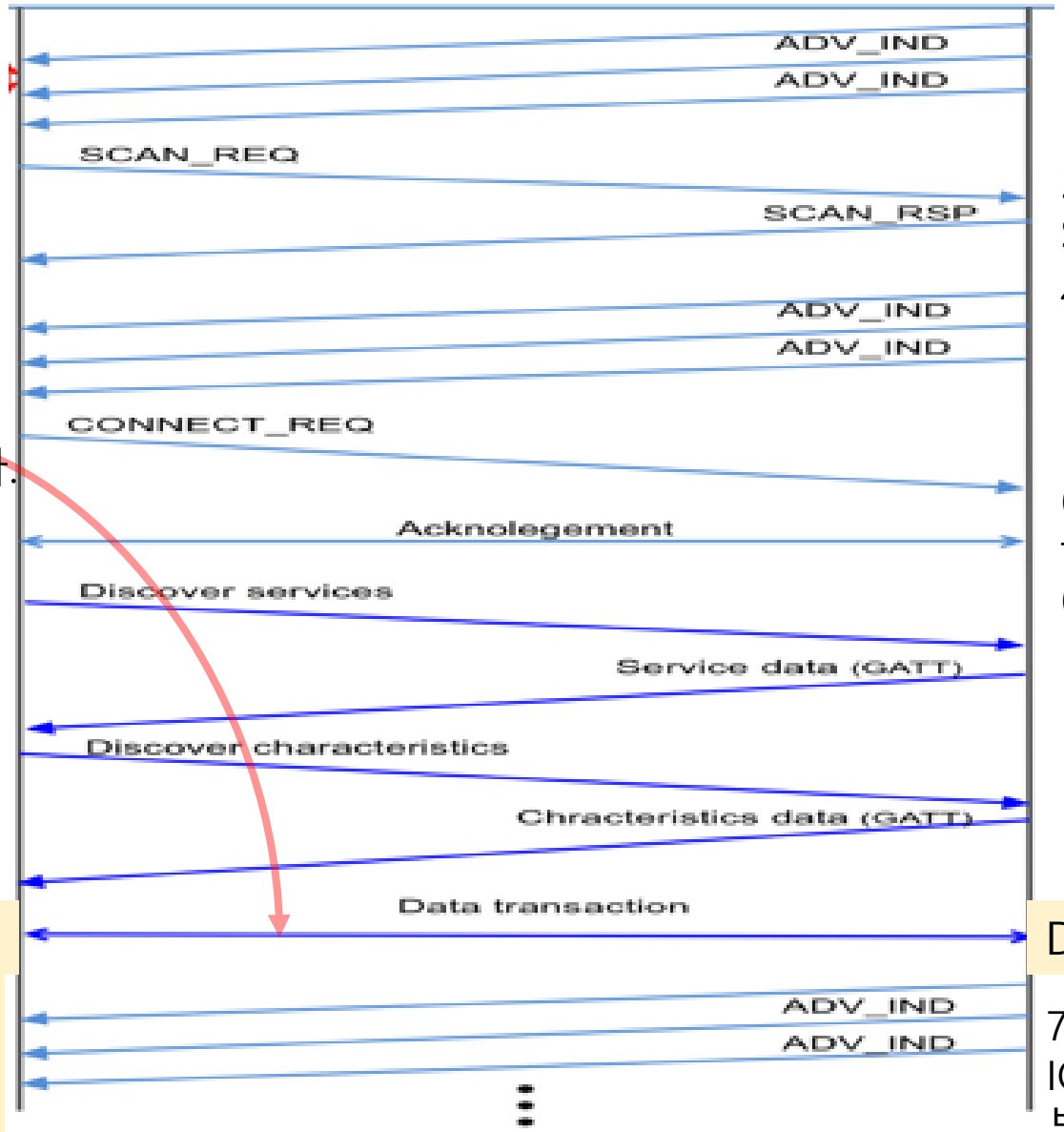
3. 해커는 평문으로 된
환자 데이터를 중간에
쉽게 탈취 가능
(MITM 공격)

해커

Ubertooth 사용하여 paket의 4 가지 정보를 추적하여 Tracking

phone

IOT device



1. IOT device가 Advertising Paket을 보낸다

2. User는 블루투스를 켠 후, IOT device의 정보를 얻기 위해 SCAN_REQ를 보낸다

3. SCAN_REQ를 받은 센서는 SCAN_RSP를 보낸다

4. Pairing이 완료되고, 센서는 다시 Advertising Packet을 다시 일정 주기마다 보낸다.

5. Phone에서 IOT device로 부터 data를 주고받기 위해 버튼을 눌러 Connection을 맺습니다. CONNECT_REQ를 보낸다

6. Acknowledging을 시작하고, timing 정보 등을 동기화 한다 (Connection 완료)

Data (FEA Encryption)

Data (FEA Encryption)

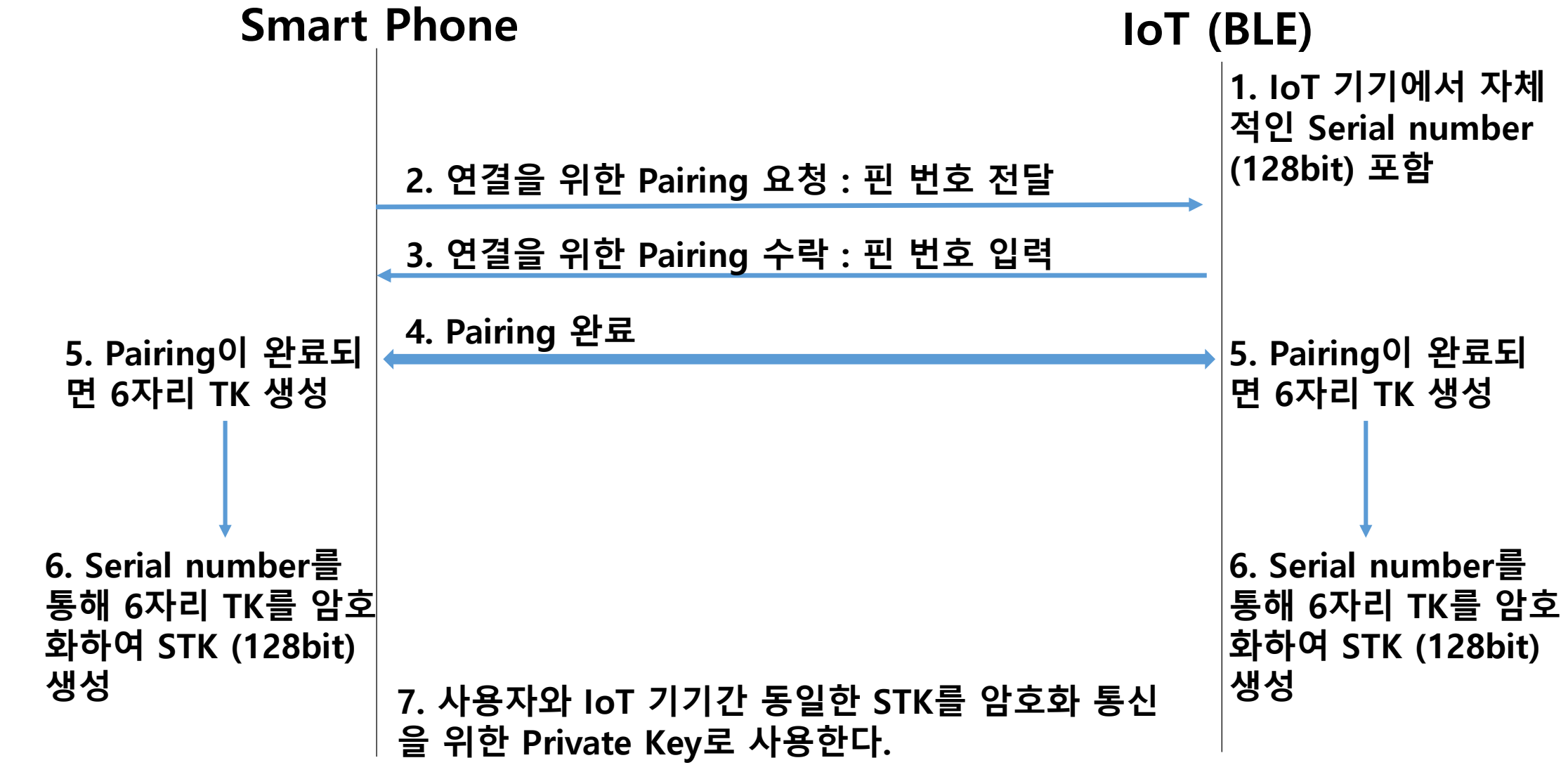
FEA, AES, LEA 중에서 작은 정보 암호화에 효율적인 FEA를 사용할 것(LUT 적용)

7. 데이터 전송이 완료되었으면 IOT device가 Advertising Paket을 보낸다 (Connection 종료)

03 | Proposal Method

Generation method of private key used for data encryption.

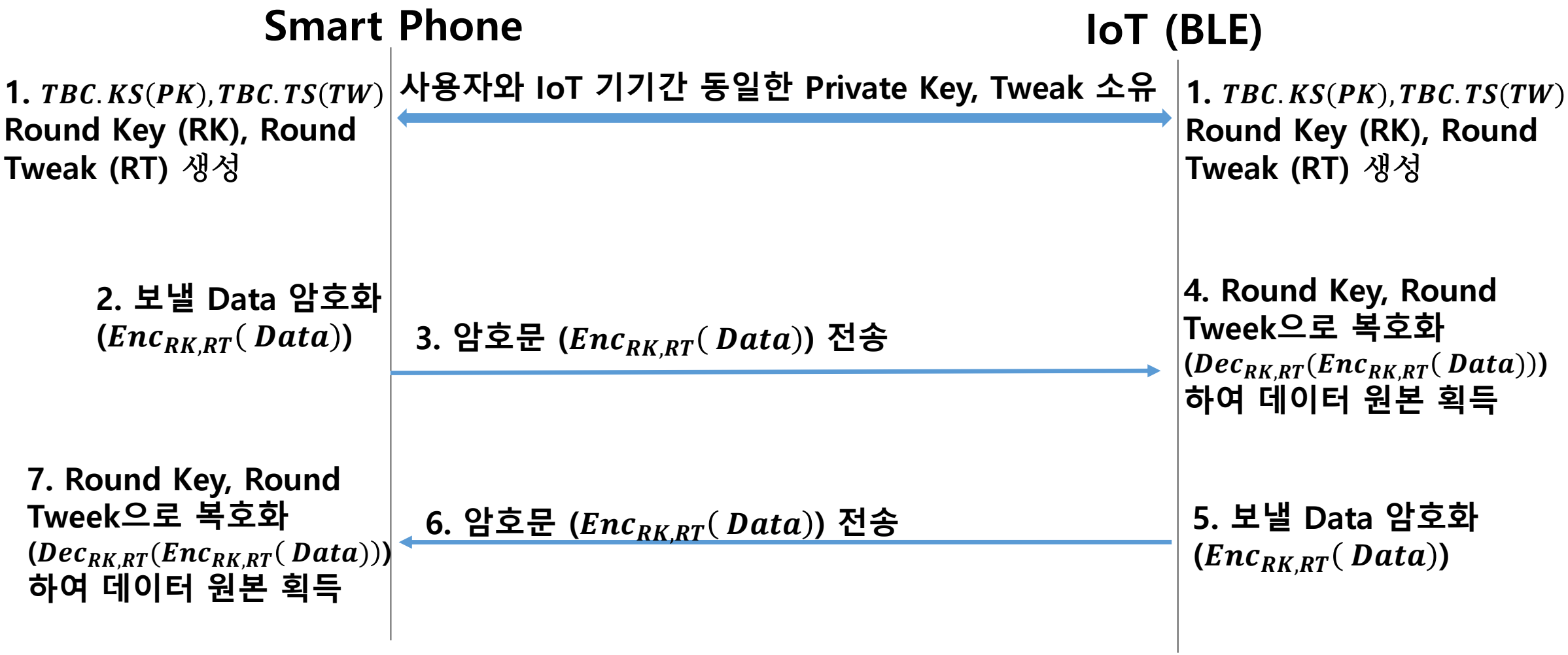
IoT와 BLE 통신에서 형태보존암호를 활용한 데이터 암호화 통신



03 | Proposal Method

Encrypted data communication between user and IoT device.

IoT와 BLE 통신에서 형태보존암호를 활용한 데이터 암호화 통신

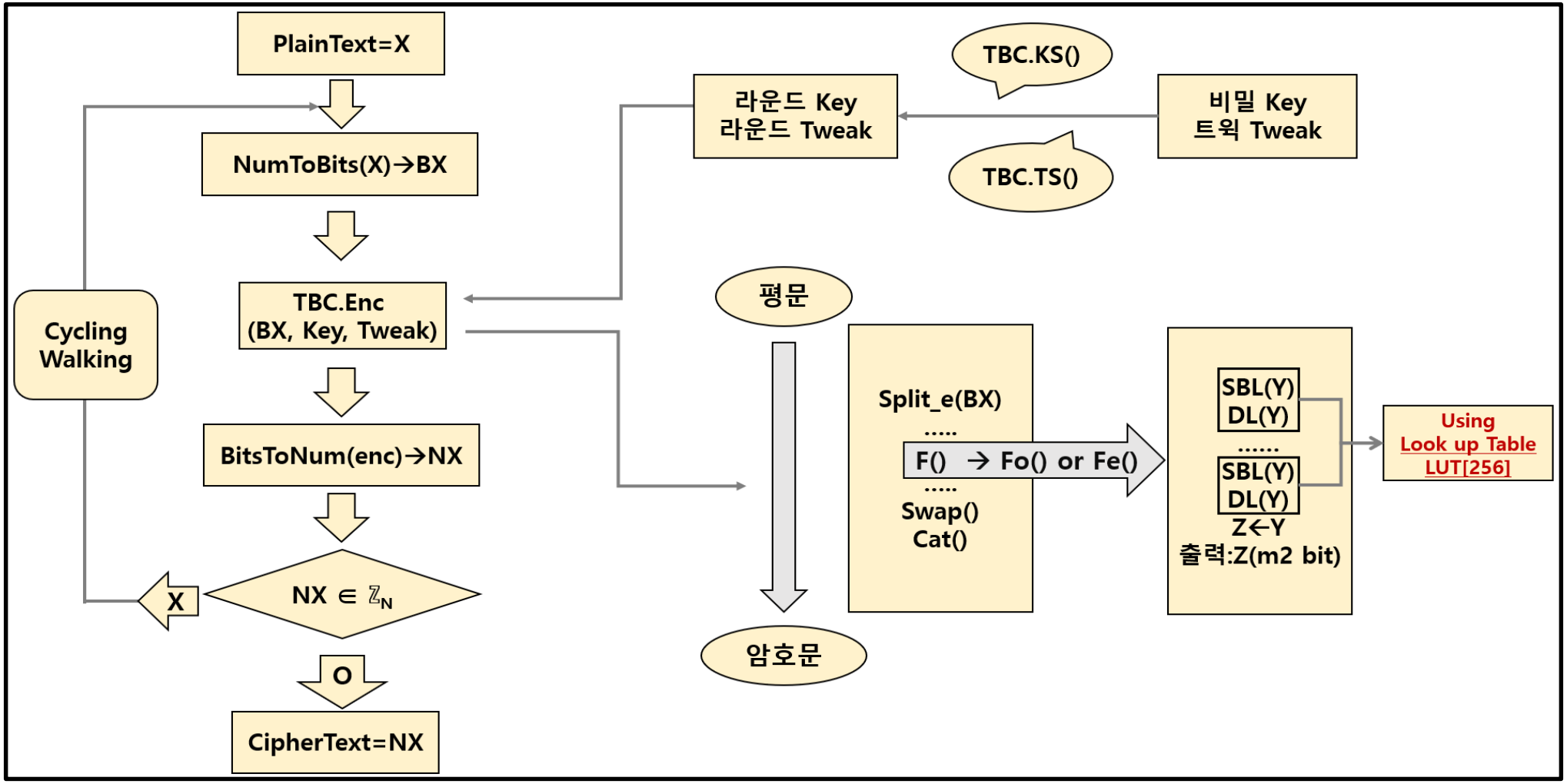


presentation

4. Apply & Evaluation

04 | Apply & Evaluation

IoT와 BLE 통신에서 형태보존암호를 활용한 데이터 암호화 통신



04 | Apply & Evaluation

IoT와 BLE 통신에서 형태보존암호를 활용한 데이터 암호화 통신

블록암호화의 비교를 위해 FEA는 4byte*4 암호화를 수행

Processor	Atmega2560 (8bit AVR)
Flash Memory	256KB
SRAM	8KB
EEPROM	4KB
Implementation Environment	Arduino IDE
FEA	Function for TBC operation type2
	Implementation based on TTA-Standard (AVR-GCC)

Test in Aduino(Mega2560)

구분	Clock Cycle
FEA	46s
FEA(Using LUT)	5.75s

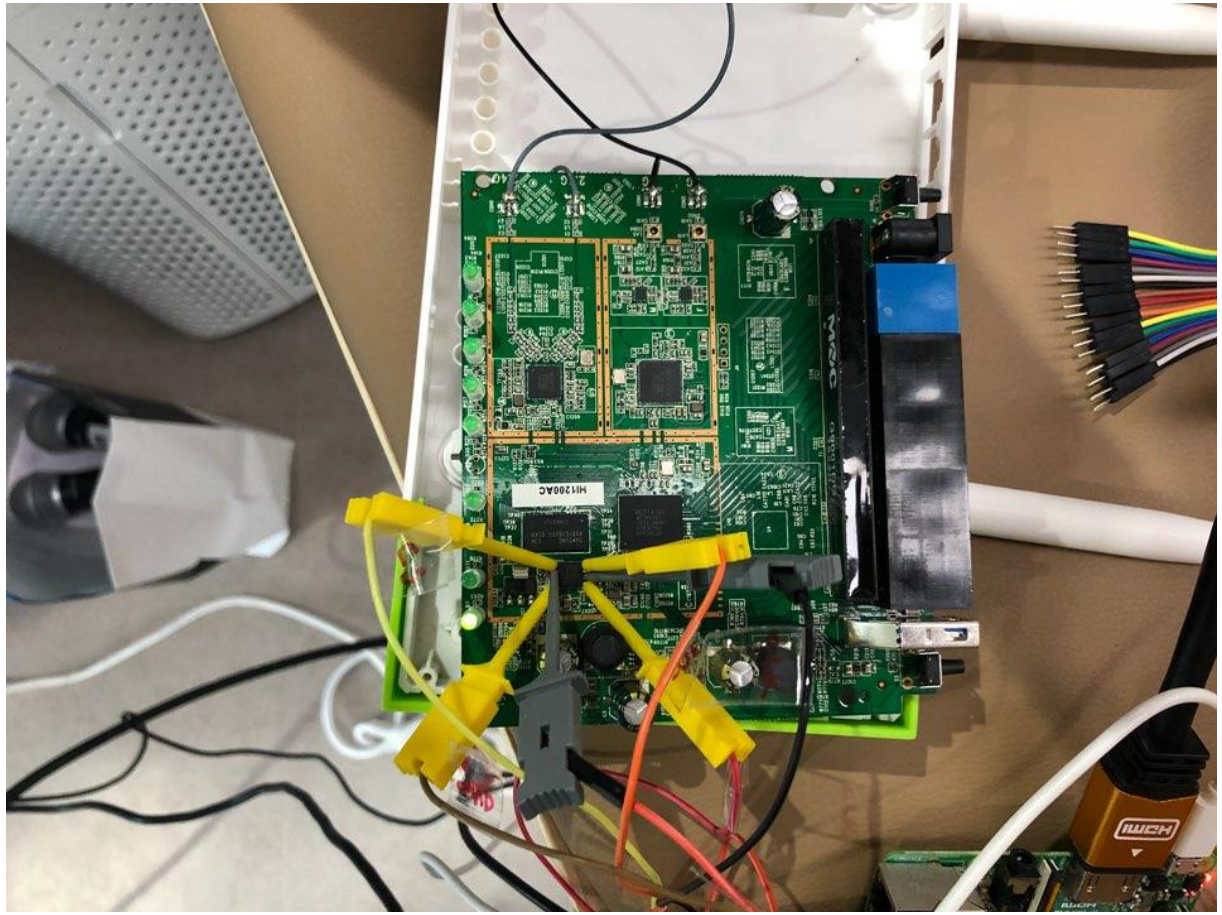
Test cases 1000개에 대해 FEA 최적화 (LUT) 전, 후 4byte 평문 암・복호화 시간 계산

presentation

5. Supplement

05 | Supplement

IoT와 BLE 통신에서 형태보존암호를 활용한 데이터 암호화 통신



임베디드 장비 취약점을 활용한 공격

1. Raspberrypi를 이용한 펌웨어 추출
2. 보통 공유기는 8핀의 Flash rom 사용

→ 각 핀의 역할을 파악 (IC 칩에 대한 정보 찾기) 후 연결

3. 명령어 입력: Sduo flashrom -p linux_spi:dev=/dev/spidev0.0 -r firmware.bin
4. 펌웨어 추출 (5~10분 소요)
5. 기존의 IoT 장비의 경우 공개키 암호화 방식이 아님으로, 펌웨어 추출을 활용하여 Srial Number 추출 가능.

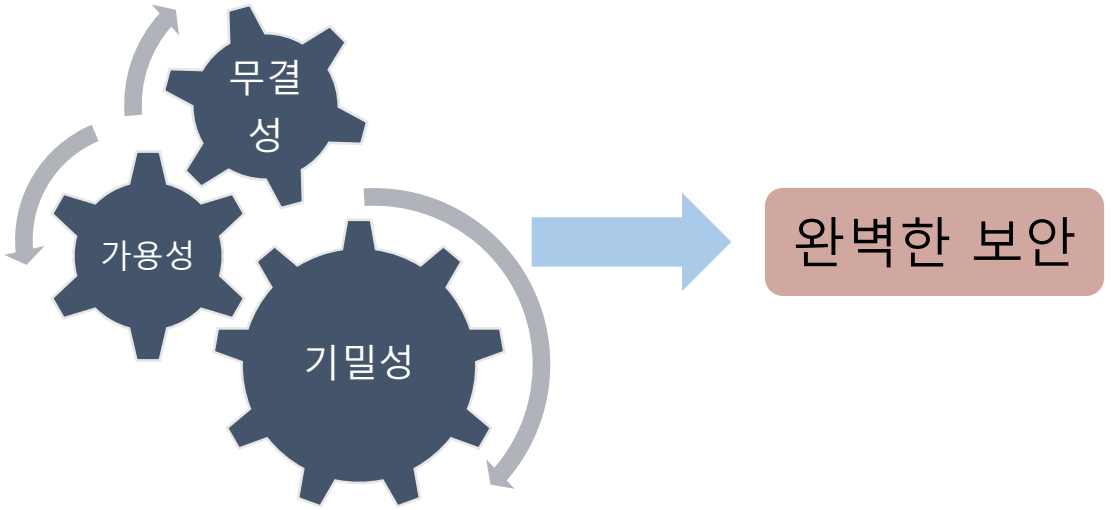
06 | Conclusion

IoT와 BLE 통신에서 형태보존암호를 활용한 데이터 암호화 통신

1) BLE를 통하여 IoT와 device 간의 통신상 보안성 문제 제기

2) 한번에 적은 양을 통신하는 IoT 무선통신 환경에서 효과적 방법 제안

3) 지난 2017년 11월 과학기술정보통신부 보도자료 [8] 에 앞으로 IoT 제품・서비스에서 데이터 암호화에 대한 대비가 필요하다고 보도하였듯이 차후 IoT 환경에서의 추가적 연구가 필요



07 | References

- [1]. Bluetooth. Bluetooth Core Specification Version 5.0 [Internet]. Available: https://www.bluetooth.com/ko-kr/specifications/bluetooth-core-specification.
- [2]. G. W. Kwon, S. H. Cho, "A Study on the vulnerability of Bluetooth Low Energy Security", in *Proceeding of the 2016 Winter Conference of the Korean Institute of Communications and Information Sciences*, vol. 59, pp. 183-184.
- [3]. M. J. Kim, "An Analysis on the Number of Advertisements for Device Discovery in the Bluetooth Low Energy Network," *Journal of the Institute of Electronics and Information Engineers*, vol. 53, no. 8, pp. 1151-1160, Aug, 2016.
- [4]. J. H. Jeon, "Study on the Security Threats Factors of A Bluetooth Low Energy," *Journal of the Korea Convergence Security Association*, vol. 17, no. 4, pp. 3-9, Oct, 2017.
- [6]. T. H. Park, H. J. Seo, G. R. Lee, H. W. Kim "Efficient implementation of simeck family block cipher on 16-bit MSP430," *2017 Ninth International Conference on Ubiquitous and Future Networks* (ICUFN), pp. 983-988 July, 2017.
- [7]. Telecommunications Technology Association. TTAK.KO-12.0275. Format-Preserving Encryption Algorithm FEA [Internet]. Available: https://tta.or.kr/include/Download.jsp?filename=choan%2F%5B2015-203%5D_%C7%FC%C5%C2+%BA%B8%C1%B8+%BE%CF%C8%A3+FEA.hwp.
- [8]. 과학기술정보통신부. (2017) "사물인터넷(IoT) 보안 인증서비스 설명회 개최". 13 Nov, 2017
- [9]. J. H. Lim, G. W. Na, J. M. Woo, and H. J. Seo, "Ransomware Prevention and Steganography Security Enhancement Technology Using Format Preserving Encryption," *Journal of the Korea Institute of Information and Communication Engineering*, vol. 22, no. 5, pp. 805-811, May, 2018

Presentation

Thanks for Watching