Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.28, NO.6, Dec 2018 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2018.28.6.1

IoT와 BLE 통신상의 형태보존암호 활용 및 최적화 구현 기법*

임 지 환,† 권 혁 동, 우 재 민, 안 규 황, 김 도 영, 서 화 정‡
한성대학교

Utilization and Optimized Implementation of Format Preserving Encryption Algorithm for IoT and BLE Communications*

Ji-hwan Lim,† Hyuk-dong Kwon, Jae-min Woo, Kyu-hwang An,
Do-young Kim, Hwa-jeong Seo‡
Hansung University

요 약

오늘날 스마트폰을 중심으로 많은 사물인터넷 (Internet of Things, IoT) 기기들이 무선으로 연결되는 데 있어서 빼놓을 수 없는 기술이 바로 블루투스이다. 또한, IoT 디바이스와 사용자 간에 블루투스 통신은 주로 Bluetooth Low Energy (BLE)를 통해서 이루어지는데, 블루투스 통신기술이 점차 발전함에 따라 기존 BLE의 보안 취약점은 더욱 두드러질 것이다. 현재까지 블루투스 접근성에 대한 연구는 꾸준히 이뤄지고 있지만, 블루투스 통신에서 데이터 보호에 대한 연구는 많이 부족하다. 따라서 본 논문에서는 IoT와 사용자 간 BLE 통신에서 데이터를 주고받을 때, 평문이 아닌 형태보존암호 (Format Preserving Encryption Algorithm, FEA)를 통해 암호문을 주고받으며 통신하기 위한 효과적 방법에 대해 제안하고, 최적화 구현한 형태보존암호에 대해 Arduino와 PC에서 직접 테스트하여 성능을 측정한다.

ABSTRACT

Bluetooth is the key technology in the wireless connection of many Internet of Things (IoT) devices, especially focused on smartphones today. In addition, Bluetooth communication between the IoT device and the user is mainly performed via Bluetooth Low Energy (BLE), but as the Bluetooth technology gradually develops, the security vulnerability of the existing BLE is more prominent. Research on Bluetooth accessibility has been conducted steadily so far, but there is lack of research for data protection in Bluetooth communication. Therefore, in this paper, when sending and receiving data in BLE communication between IoT and users, we propose effective methods for communicating with each other through the Format Preserving Encryption Algorithm (FEA), not the plain text, and measures performance of FEA which is optimized in Arduino and PC.

Keywords: Internet of Things (IoT), Bluetooth Low Energy (BLE), Format Preserving Encryption Algorithm (FEA)

Received(09. 27. 2018), Modified(11. 26. 2018), Accepted(11. 26. 2018)

* 본 논문은 2018년도 한국정보보호학회 영남지부 학술대회에 발표한 우수논문을 개선 및 확장한 것임. 이 성과는 부분적으로 2018년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. NRF-2017R1C1B5075742) 그리고 본 연구는 부분적으로 과학기술정보통신부 및 정보통신기술진흥센터의 대학 ICT 연구센터 육성지원사업의 연구결과로 수행되었음(2014-1-00743).

† 주저자, jhim147605@gmail.com
‡ 교신저자, hwajeong84@gmail.com(Corresponding author)

I. 서 론

블루투스 (Bluetooth)는 휴대기기를 서로 연결해 정보를 교환하는 단거리 무선통신 기술로서, 최신 IoT 기술에서는 여러 분야에 걸쳐 블루투스가 다양한 용도로 사용되는 추세이다. IoT의 Bluetooth 통신으로는 BLE를 사용하여 통신한다. BLE란 기존의 Bluetooth Classic보다 훨씬 적은 전력을 사용하여 Classic과 비슷한 수준의 무선 통신을 할 수 있다는 점이다. 이로 인해 다양한 IoT 디바이스들이 개발될 수 있는 원동력이 되었다. 현재 BLE를 사용한 IoT 통신은 비콘, 다중 IoT 센서 연결 또는 IoT와 사용자 간에 직접 통신 등에 사용되고 있다.

2016년에 Bluetooth SIG (Special Interest Group)는 6년 만에 블루투스 5.0을 선보여 기존 Bluetooth 4.0보다 통신 거리 4배, 통신속도 2배, Pairing 문제 해결 등 기존보다 진보된 무선통신 기술을 내놓았다 [1]. 하지만 이에 단점으로 기존의 블루투스 보안상 취약점이 많아 다양한 블루투스 공격 형태가 존재한다는 것이다[2]. 블루투스 접근 상 문제도 WI-PI 보안의 WPA2 보안보다 취약하다. 또한, 아직 BLE 통신에서는 무결성, 가용성 이외에 통신하는 데이터를 보호하는 기밀성 연구의 진행이 매우 저조하여, 기술의 발전에 비교하면 데이터의 보안성이 매우 취약한 상태이다. 따라서 본 논문에서는 BLE 통신에서 IoT 센서와 사용자가 통신할 때, 데이터 보안을 위주로 정보의 기밀성 강화에 대한 방법을 제안하고 형태보존암호 최적화 구현 기법도 설명하고자 한다.

본 논문의 구성은 다음과 같다. 2장은 관련 연구 동향에 대해 소개하며 3장 본론에서 제안기법에 대해 설명한다. 그리고 4장에서 IoT 환경에서 제안 기법에 대한 성능 평가 및 형태보존암호 최적화에 따른 PC에서 성능까지 측정한다. 마지막 5장에서 본 논문의 결론을 맺도록 한다.

II. 관련 연구 동향

2.1 BLE 통신 연구 동향

최근 IoT와 스마트 디바이스 간의 통신에 대한 보안이 중요하게 떠오르고 있다. 또한, 블루투스 무선통신상에서 연결 부분에 대한 보안 기술 관련 취약점이 발견되고 있다 [3]. 그리고 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 [4]. 그림 1은 원격 의료서비스에 대한 공격으로 사용자가 애플리케이션으로 로그인 시 아이디, 비밀번호를 포함한 중요 정보가 공격자에게 평문으로 전송되는 취약점을 악용해, 사용자의 개인정보뿐만 아니라 정보를 바탕으로 병원의 의료정보에 대해서도 가로챌 수 있는 문제점을 보여준다. 사용자의 의료정보는 개인정보 중에서도 개인의 생명과 즉결된 정보이다. 이와 같은 위험성을 제거하고 사물인터넷 제품과 모바일 앱의 연동이 활성화되기 위해 2017년 11월 말부터 과학기술정보통신부와 한국인터넷진흥원에서 사물인터넷 보안 인증서비스를 시행했다.

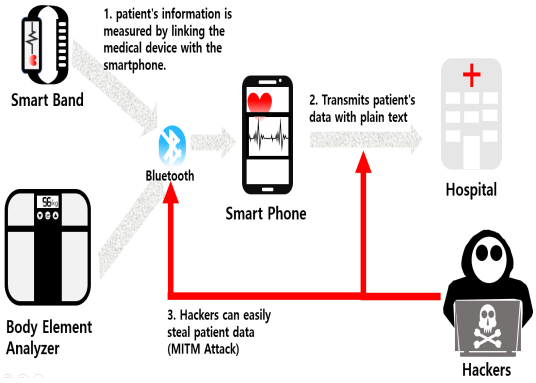

Fig. 1. Infringible scenario through hacking of hospital information system [5]

2.2 형태보존암호 최적화 연구 동향

국내에서 독자적으로 개발한 Format-Preserving Encryption Algorithm (FEA) 암호기술은 NSRI에 의해 개발되었다. 이는 NIST에서 개발해 표준으로 등록된 FPE의 Feistel 구조와 다른 트위커블 (Tweakable) 가변 길이 블록암호의 특징을 갖는다 [6]. 형태보존암호 (FEA) 최적화 구현 연구로는 [7, 8] 논문에서 수행한 결과가 있다. [7]에서는 여러 플랫폼 환경에서 FEA에 대하여 구현하였고, i5-4590 3.3GHz 환경에서 FEA-2에 대하여 Key Scheduling과 8byte Encrypt 1회 수행 기준 0.007ms의 시간이 측정되고, [8]에서는 단일 플랫폼 i5-6200U 2.3GHz 환경에서 구현하였

고, FEA-2에 대하여 Key Scheduling, 8byte Encrypt, 8byte Decrypt를 수행하여 1회 수행 기준 0.005ms의 시간이 측정되었다. 또한, [8]에서 경량암호 LEA 보다 2.6배가량 빠르게 구현하여 형태보존암호의 속도 측면에서도 준수함을 보였다.

2.3 BLE 통신 패킷 분석

블루투스 통신은 유선을 통한 데이터 전송을 뛰어넘어 저전력 무선을 활용한 데이터 전송으로 많이 활용되었으며 현재 산업의 많은 부분에 사용되고 있다. 하지만, 블루투스 통신은 상호 데이터 교환을 위한 초기 연결과정 (Connection)을 제외하면 데이터를 주고받는데, 암호화를 전혀 사용하지 않기 때문에, Packet Sniffing 공격에 매우 취약하다. 현재 Packet Sniffing 코드는 Github 검색을 통해서도 쉽게 찾을 수 있다. BLE Packet의 구조는 그림 2와 같으며 패킷은 Preamble로 시작한다. Access Address는 32bit로 링크 계층에서 연결용 주소로서 두 장치 간에 링크 연결 시마다 달라진다. 연결 시마다 AA가 달라지더라도, 패킷의 암호화가 적용되어있지 않음으로 Reply Attack도 가능할 것으로 보인다. 제어하고자 하는 명령은 PDU 명령을 통해 제어하는데, Header와 Payload로 구성된다. Header는 PDU (Header, Payload)의 타입과 길이를 명시하고, Payload는 전송하는 데이터를 나타낸다. 또한, Payload는 Advertising address와 Advertisement Data를 포함하는데, Advertising address는 MAC address이고, Advertisement Data가 실제로 전송하는 데이터이다. 이는 최대 31바이트이다.

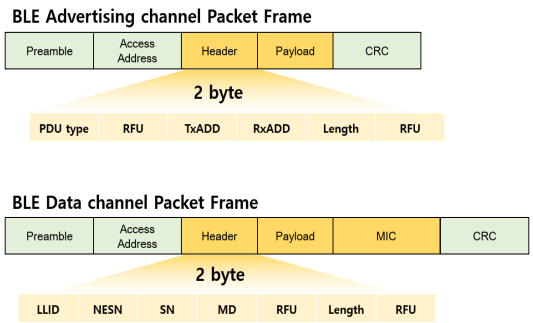

Fig. 2. BLE packet frame

III. 본 론

3.1 형태보존암호화를 통한 BLE 암호화 통신

본 절에서는 BLE 통신에서 IoT와 사용자 간에 암호화 통신을 할 수 있도록, 그림 3의 형태보존암호를 적용한다.

블루투스는 노드와 컨트롤러 간에 Connection을 통해 통신 링크가 형성된 이후에는 전송하는 패킷을 암호화하지 않는다. 따라서 공격자는 Sniffing을 수행할 수 있으므로 정보의 기밀성이 매우 떨어진다. 암호화되지 않은 패킷의 Sniffing이 가능하다면 공격자는 탈취한 패킷 내부의 사용자 장치의 MAC 주소 등 주요 정보를 탈취할 수 있고, Reply Attack 등 사회 공학적 기법을 추가하여 공격할 수 있는 루트가 다양해진다. Bluetooth 5.0 이전 버전에 대해서는 공격자가 페어링 과정부터 Sniffing으로 개입하면 키를 탈취할 수 있었지만, Bluetooth 5.0 버전은 공개키 암호를 사용하여 키를 교환함으로 탈취하기 어렵다. 키를 교환하는 과정에서는 보안성이 갖춰지지만, 결과적으로 패킷에 대해서 암호화를 수행하지는 않기 때문에 Sniffing, 컨트롤러와 연결된 노드의 펌웨어 추출, ARP Spoofing을 활용한 MITM 등에 대해서는 여전히 취약점으로 남아있다.

그림 4를 통해 사용자와 IoT 기기 간 암호화 통신을 위한 Private Key 생성하는 방식을 소개하고, 그림 5에서 생성한 Private Key를 활용하여 사용자와 IoT 기기 간 암호화 통신을 설명한다.

먼저 그림 4의 방식은 IoT 기기에서 초기 설정된 Serial Number (128bit)를 갖고 있다(1). (2,3,4) 과정을 통하여 사용자와 IoT 기기 간

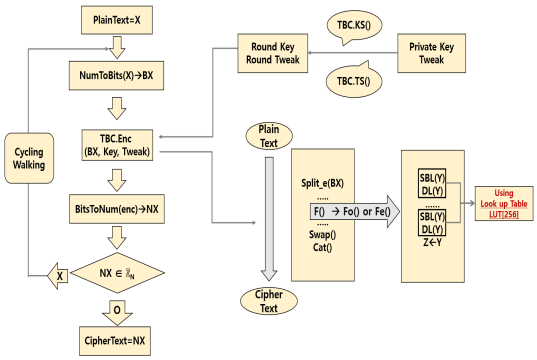

Fig. 3. Implementation process of Format Preserving Encryption Algorithm

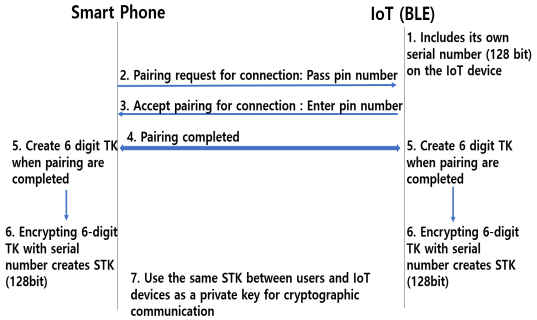

Fig. 4. Generation method of private key used for data encryption

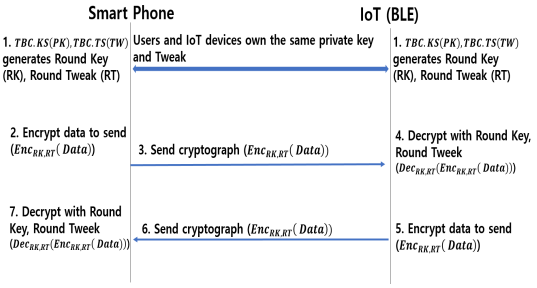

Fig. 5. Encrypted data communication between user and IoT device

Pairing이 완료되면, 양 측에 동일한 6자리의 TK가 생성된다(5). 양 측에서 Serial Number를 Private Key로 사용하여 TK를 암호화하여 STK (128bit)를 생성한다(6). 최종적으로 사용자와 IoT 기기 간 동일한 STK를 암호화 통신을 위한 Private Key로 사용한다.

그림 5는 통신할 데이터를 암호화하기 위해서 그림 4에서 생성한 Private Key를 FEA의 TBC.KeyScheduling, TBC.TweakSchduling 함수로 Round Key (RK), Round Tweak (RT)를 생성한다(1). 최종적으로 (2,3,4) 과정은 사용자가 데이터를 보낼 때 암호화하여 보내고 IoT에서 복호화하는 모습이고, (5,6,7) 과정은 IoT에서 사용자에게 암호화하여 데이터를 보내고, 사용자는 복호화하여 데이터 원본을 받는 모습이다.

3.2 형태보존암호화 최적화 구현

본 절에서는 형태보존암호 구현 방법과 최적화 방안에 대해 설명하고자 한다. 형태보존암호의 전체 구현 과정은 그림 3와 같고, 암·복호화 구조는 Tweak 적용 블록 암호 TBC의 암·복호화를 기반으로 한 Cycle-Walking이다. 또한, 암·복호화 과정에서 항상 랭킹함수 (NumToBits(), BitsToNum(), StrToNum(), NumToStr())를 통과한다. 암호화 함수 (FEA.Enc())는 평문 (p), 비밀 키 (K), 트윅 (T)를 입력으로 하여 암호문 (c)를 출력하며, 복호화 함수 (FEA.Dec())는 암호문 (c), 비밀 키 (K), 트윅 (T)를 입력으로 하여 평문 (p)를 출력한다. 형태보존암호의 복호화 과정은 암호화 과정의 라운드를 반대로 수행하는 과정이다. 형태보존암호의 암·복호화 과정은 수식으로 (1, 2)와 같이 기술할 수 있다.

$$FEA_N.Enc(K,T,X) = CW(TBC_n.Enc(TBC_n.KS(K), TBC_n.TS(T), \cdot), Z_N)(X) \quad (1)$$

$$FEA_N.Dnc(K,T,X) = CW(TBC_n.Dnc(TBC_n.KS(K), TBC_n.TS(T), \cdot), Z_N)(X) \quad (2)$$

또한, 암·복호화 시 매번 사용되는 랭킹함수에 대해서 영어 알파벳 26진수의 비효율성에 착안하여 이를 32진수로 변환 (Padding)하여 Division (a / 26) 연산은 표 1의 Shift (a 〉〉 5) 연산으로 대체하고, Modular (a % 26) 연산은 표 2의 And (a & 0x1f) 연산으로 대체하였다. 그림 6은 표 6 환경에서 Shift (a 〉〉 5), Modular (a % 26) 연산에 대해 테스트케이스 1억 번 수행한 결과이다. 또한, 영문자 소문자, 대문자, 숫자를 다 사용할 시에는 62진수를 사용하게 되는데, 이에 대해서는 64진수로 패딩 하여 사용하면 사용하고자 하는 글자 수 1~15자리까지 동일한 비트 수가 사용됨을 알 수 있다. 이는 짧은 길이 암호화에 특성을 갖는 형태보존암호에 효과적이다.

형태보조암호에서 큰 비중을 차지하고 있는 Cycle-Walking 과정은 암호화 수행 후 조건 ($C \in Z_N$)이 일치하면 암호문으로 일치하지 않으면 랭킹함수부터 암호화 과정을 다시 수행하게 된다. 이는 암호화를 1번 수행하면 flag 값을 1로 설정하여 flag가 1이면 재 암호화 과정에서 모든 라운드를 전부 수행하지 않고, 1라운드를 수행 후 Cycle Walking을 통해 재검증을 받는 방식을 사용하면

Table 1. Optimize division operation using shift operation

```
// Replace with >>5 operation
temp = a >> 5;
mov         eax, dword ptr
mov         edx, dword ptr
mov         cl, 5
call        _aullshr (0BE1230h)
mov         dword ptr, eax
mov         dword ptr, edx
```

Table 2. Optimize Modular operation using and operation

```
// Replace with &0x1f operation
temp = a & 0x1f;
mov         edx, dword ptr
and          edx, 1Fh
mov         eax, dword ptr
and          eax, 0
mov         dword ptr, edx
mov         dword ptr, eax
```

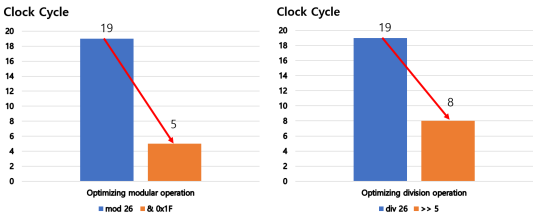

Fig. 6. Test cases 100 million modular, division operation optimization result

더 효과적이다. 복호화 과정 또한 암호화 과정과 마찬가지로 기존 라운드를 전부 수행 후, 조건이 일치하면 그대로 복호문으로 나오지만 일치하지 않으면 flag 값을 1로 설정하여 재 복호화 과정에서 모든 라운드를 수행하지 않고 1라운드 수행 후, Cycle-Walking을 통과하는 방법으로 검증할 수 있다.

IV. 성능 평가

본 장에서는 Arduino Mega에서 구현한 128bit의 키 길이를 갖고, 제 2형 TBC로 구현한 형태보존암호의 성능을 평가한다. 또한, PC에서 구현한 128, 192, 256bit의 키 길이를 갖고, 제 2형 TBC로 구현한 형태보존암호의 성능까지 비교하고자 한다.

Arduino Mega에서 구현 및 테스트 환경은 표 4과 같다. 구현은 형태보존암호 TTA 표준[6]을 참조하여 구현하였고, [8]의 Look Up Table (LUT) 2KB 방식을 사용하여 형태보존암호의 치환(SBL)과 확산 (DL) 함수를 최적화하였다. 표 5는 테스트 케이스 1000개 (그림 3의 FEA 전 과정 수행)에 대한 4byte 평문 암·복호화 속도를 비교한 표이다. Arduino에서 LUT (2KB)를 사용한 결과 최적화 전보다 8배 정도 속도가 향상된 것을 확인할 수 있다. 본 논문에서의 테스트는 Arduino Mega 2560에서 수행했으므로, SRAM이 8KB로 LUT 2KB를 업로드해도 문제없이 실행할 수 있지만, ATmega328로 실험할 경우 SRAM이 2KB이므로, 프로그램 코드와 LUT (2KB)를 전부 업로드 할 수 없다. 따라서 이러한 경우 SRAM 보다 용량이 큰 Flash Memory에 LUT (2KB)를 저장하고 읽어오면 된다 [9]. 표 3는 Flash Memory에 저장하고, 읽어오는 간략한 테스트 방법을 나타낸다.

PC에서 구현 및 테스트 환경은 표 6와 같다. PC에서의 구현도 위와 마찬가지로 [6, 8]을 참조하여 구현하였고, 본 논문의 최적화 기법을 추가로 적용하였다. 표 7은 128, 192, 256bit의 키 길이를 갖는 테스트 케이스 1000개에 대해 각각 8byte 평문을 암·복호화하여 속도를 비교한 표이다. 본 논문에서 테스트한 성능 평가 결과는 그림 3의 전 과정을 1000회 수행하였을 때 시간을 나타내며, 그 결과

Table 3. Test for read and write from flash memory

```
#include <avr/pgmspace.h>

const uint8_t save[] PROGMEM = { 0x01,
0x02, 0x03, 0x04, 0x05 };
int k;
void setup() {
  Serial.begin(9600);
}
void loop() {
  for(k = 0; k < 5; k++)
    Serial.print(pgm_read_byte_near(save+k));
}
```

Table 4. Test Environment for Arduino and Program

Processor	ATmega2560 (8 bit AVR)
Flash Memory	256KB
SRAM	8KB
EEPROM	4KB
Implementation Environment	Arduino IDE
FEA	Functions for TBC operation type 2
	Implementaion based on TTA-Standard and Optimization of SBL, DL Function (AVR-GCC)

Table 5. FEA performance improvement in 4byte encryption and decryption before and after using LUT in 1,000 test cases

Method	**FEA**	**FEA (LUT)**
Timing	46 sec	5.75 sec

Table 6. Test Environment for PC and Program

Processor	Intel Core i5-8250U CPU 1.6 GHz
Memory	8GB (DDR4)
Operation System	Windows 10
Implementaion Environment	Microsoft Visual Studio C++ 2010 Express x64 tools
Optimized Compile Options	O2
FEA	Functions for TBC operation type 2
	Implementation based on TTA-Standard and Optimization of SBL, DL Function, Ranking Function, Cycle-Walking (C Language)

[7, 8]의 테스트 결과보다 더 빠른 성능임을 확인할 수 있다.

Table 7. FEA performance improvement in 8byte encryption and decryption before and after optimization in 1,000 test cases

Operation Mode	**Timing**
FEA_128	0.052 sec
FEA_128_Opt	0.006 sec
FEA_192	0.060 sec
FEA_192_Opt	0.008 sec
FEA_256	0.067 sec
FEA_256_Opt	0.007 sec

V. 결 론

본 논문에서는 사물인터넷 BLE 무선통신 환경에서 무결성, 가용성 측면보다 연구 진행이 저조한 데이터 기밀성 측면에서 형태보존암호를 활용하여 이를 효과적으로 보완하는 방식을 제안하였다. 기존의 블록 암호는 데이터를 암호화하면 크기가 늘어나지만, 형태보존암호를 사용하면 평문과 암호문의 크기와 길이가 일치하기 때문에 데이터베이스 활용도 또한 매우 효과적이고, 한 번에 적은 양의 데이터를 보내는 BLE 통신에서 암호화하여도 데이터의 크기가 늘어나지 않는다는 매우 큰 장점이 있다. 또한, 8bit-AVR Arduino Mega 2560에서 형태보존암호를 AVR-GCC로 최적화 구현하여 성능 평가를 수행하고, SRAM 용량이 작은 환경에서 효과적으로 메모리를 관리하는 방법에 대해 간략히 설명하였다. PC 환경에서 구현한 형태보존암호는 128, 192, 256bit의 키 길이 각 환경에서 최적화 구현하여 성능을 평가하였다. 향후 블루투스 분석을 추가로 수행하여 실제 노드 장비의 해킹을 통하여 보안성을 점검할 예정이고, 추가로 Spoofing Tool까지 구현하고자 한다.

References

[1] Bluetooth. Bluetooth Core Specification Version 5.0 [Internet]. Available: https://goo.gl/44Gbpf

[2] KISA. BlueBorne Bluetooth attack related security update recommended [Internet]. Available: http://bitly.kr/mKku

[3] 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

〔4〕 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 Infornation Engineers*, vol. 53, no. 8, pp. 1151-1160, Aug, 2016

〔5〕 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〕 Telecommunications Technology Association. TTAK.KO- 12.0275. Format-Preserving Encryption Algorithm FEA 〔Internet〕. Available: https://goo.gl/TVx3Y7

〔7〕 C. H. Park, S. Y. Jeong, D. W. Hong and C. H. Seo, "Optimal

〔8〕 Implementation of Format Preserving Encryption Algorithm FEA in Various Environments," *Journal of the Korea Institute of Information Security & Cryptology*, Vol. 28, No. 1, pp. 41-51, 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

〔10〕 Arduino. Arduino PROGMEM Manual 〔Internet〕. Available: https://www.arduino.cc/reference/en/language/variables/utilities/progmem/

〈저자소개〉

임 지 환 (Ji-hwan Lim) 학생회원
2014년 3월~현재: 한성대학교 IT 융합공학부 학부과정(3학년)
2018년 7월~현재: 차세대 보안리더 양성과정(Best of the Best 7th)
〈관심분야〉 무선해킹, IoT, Z-Wave 프로토콜, 암호구현

권 혁 동 (Hyuk-dong Kwon) 정회원
2018년 2월: 한성대학교 정보시스템공학과 졸업
2018년 3월~현재: 한성대학교 정보시스템공학과 석사과정
〈관심분야〉 블록체인, 모바일 보안, 암호구현

우 재 민 (Jae-min Woo) 학생회원
2014년 3월~현재: 한성대학교 IT 융합공학부 학부과정(3학년)
〈관심분야〉 IoT, 데이터 통신보안

안 규 황 (Kyu-hwang An) 학생회원
2018년 2월: 한성대학교 IT 융합공학부 졸업
2018년 3월~현재: 한성대학교 정보시스템공학과 석사과정
2018년 3월~2018년 10월: 국가 암호기술 전문인력 양성과정 수료
〈관심분야〉 블록체인, 블록암호, IoT 보안, Hash 함수

김 도 영 (Do-young Kim) 학생회원
2014년 3월~현재: 한성대학교 IT 융합공학부 학부과정(3학년)
〈관심분야〉 모의해킹, 보안솔루션

서 화 정 (Hwa-jeong Seo) 종신회원
2010년 2월: 부산대학교 컴퓨터공학과 학사 졸업
2012년 2월: 부산대학교 컴퓨터공학과 석사 졸업
2012년 3월~2016년 1월: 부산대학교 컴퓨터공학과 박사 졸업
2015년 4월~5월: 난양공대 인턴쉽
2016년 1월~2017년 3월: 싱가포르 과학기술청
2017년 4월~현재: 한성대학교 IT 융합공학부 조교수
〈관심분야〉 정보보호, 암호화 구현, IoT