양자 내성 암호를 적용한 블루투스 모델 제안

양유진*, 장경배*, 송경주*, 김현지*, 오유진*, 서화정+*
*한성대학교 IT융합공학부
yujin.yang34@gmail.com, starj1023@gmail.com, thdrudwn98@gmail.com,
khj1594012@gmail.com, oyj0922@gmail.com, hwajeong84@gmail.com

Proposal of Bluetooth model with Post-Quantum Cryptography

Yu-Jin Yang*, Kyung-bae Jang*, Gyeong-ju Song*, Hyun-Ji Kim*,
Yu-Jin Oh*, Hwa-Jeong Seo+*
*Dept. of IT Convergence Engineering, Han-Sung University

요 약

IoT 기기가 발전으로 블루투스 활용도와 보안에 대한 관심이 증가하면서, 블루투스와 관련된 취약점이 매년 발생하고 있다. 보안을 높이기 위하여 블루투스 4.2 버전부터 페어링 단계에서 타원곡선 디피-헬먼 키 교환을 적용하였지만 타원곡선 기반의 암호들은 양자컴퓨터의 발전과 Shor 알고리즘에 의해 더 이상 안전하다고 보기 어렵다. 본 논문에서는 양자 환경에서 발생할 법한 블루투스 관련 취약점을 미연에 방지하기 위하여 페어링 단계에 적용된 기존의 암호 대신 양자 내성 암호 NewHope를 적용한 블루투스 모델을 제안한다.

1. 서론

무선이어폰, 웨어러블 기기 등 IoT기기가 발전됨에 따라 블루투스의 활용도가 점점 확대되고 있다. 2021년, COVID-19이 계속되고 있어 경기가 어려운 시점에도 연평균 10%의 성장률을 보일정도로 블루투스는 다양한 분야에서 사용되고 있다. 그에 따라 블루투스와 관련된 취약점도 매년 지속적으로 발생하고 있는 실정이다[1]. 2017년, 블루투스가 활성화된 기기에 접근하여 악성코드를 배포하는 블루본(BlueBorne)이 발견됐고[2], 올해 5월엔 ANSSI 연구진에 의해 Blue Mirror라 불리는 취약점들이 발견됐다[3]. 그 밖에도 BIAS, BLURtooth, KNOB 등 다양한 취약점들이 발견됐다.

블루투스 4.2 이전 사양에서 주로 발생했던 레거시 페어링 관련 취약점의 경우, 타원곡선 디피-헬먼 키 교환(Elliptic-curve Diffie- Hellman, ECDH)을 적용하여 해결하였다. 그러나 현재 구글, IBM 등 여러 기업에서 개발하고 있는 양자컴퓨터와 Peter shor 교수가 제안한 Shor 알고리즘 이용하면 지수시간이 소요되던 소인수분해 문제가 다항시간 안에 해결되기 때문에 타원곡선 이론에 기반한 ECC암호와 ECDSA, ECDH 등이 더 이상 안전하지 않게 된다. 이는 양자환경에선 블루투스 보안 연결에 적용된 ECDH 키 교환 방식이 더 이상 안전하지 않음을 시사한다. 이에 기존의 암호 키 교환 방식을 대신한 양자 내성 암호의 적용이 필요하다.

본 논문에서는 2장에서 관련연구로 블루투스 연결과정과 ECDH, 격자기반암호를 적용한 키 교환 알고리즘 NewHope에 대해 살펴보고 3장에서 제안 기법을 설명하며 4장에서 결론을 맺는다.

2. 관련 연구

2.1 블루투스

스마트 워치와 같은 웨어러블 기기와 무선이어폰, 홈 IoT 제품 등에 자주 사용되는 블루투스는 2.4GHz 대역을 사용하는 무선 통신 기술이다. 블루투스의 표준 기술로는 BR/EDR(Basic Rate/Enhanced Data Rate)이라고 불리는 Bluetooth Classic과 BLE(Bluetooth Low Energy)가 있고 현재, 버전 5.3까지 개발되었다. 공격 방법으론 수동 도청(passive sniffing)과 MITM(Man-In-The-Middle, 중간자 공격)이 대표적이다.

블루투스 연결과정은 다음과 같다. 디바이스 연결까지 질의 신호를 이용하여 연결할 장치를 찾는 Inquiry, 연결을 진행하는 connecting, 연결이 완료된 후 4가지의 모드를 유지하는 connection 과정을 거친다. connecting 과정에서 페어링(pairing)을 거치

+ 교신저자 : 서화정(hwajeong84@gmail.com)

면, pairing process에 페어링에 사용된 key를 저장하는 본딩(Bonding)을 거쳐 장치가 재연결할 때 다시 페어링 과정을 거치지 않도록 한다.

한 쌍으로 만든다는 의미를 가진 페어링 단계는 크게 3단계로 볼 수 있다.

1) 페어링 기능 교환

1단계에서는 Pairing Request와 Pairing Response 패킷을 이용하여 IO(Input/Output)기능, 보안기능을 교환한다. 해당 패킷에는 요청, 응답 여부를 결정하는 Code, 입출력 유무를 결정하는 IOCap, 본딩이 유무를 나타내는 Bonding, BLE 보안 연결 페어링 요청을 위한 SC 등 총 11개의 Flag가 담겨 있다.

2) 키 생성 및 교환

2단계에서는 암호화 통신을 사용하기 위하여 키를 생성하고, 통신하고자 하는 두 기기가 생성된 키를 교환한다. 키 교환에 사용되는 기술론 LE LP(Low Energy Legacy Pairing)과 보안 단순 페어링(Secure Simple Pairing, SSP), LE 보안 연결 페어링(Secure Connection Pairing, SCP)이 있다.

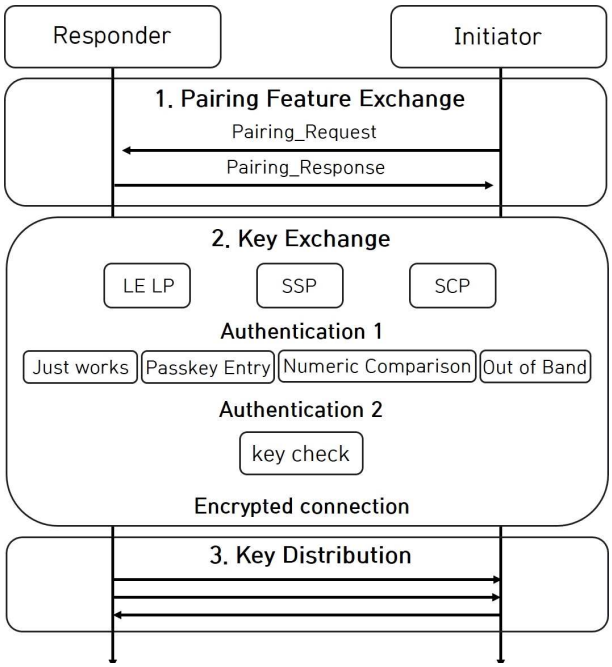
SSP와 SCP 모두 ECDH을 이용하여 키를 교환하는데 SSP는 192-bit 혹은 256-bit 크기의 키를 공유하고, SCP는 256-bit 크기의 키를 공유한다. LE LP의 경우, 위 두 가지 방식과 달리 임시키(Temporary Key, TK)와 난수 생성(Random Number Generation, RNG), 단기키(Short-term Key, STK)를 이용한 독자적인 키 교환 방식을 사용한다.

이후, Just Works, Passkey Entry, Numeric Comparison, OOB(Out-of-Band)까지 총 4가지 종류의 인증방법 중 1가지 방법을 선택하여 MITM 공격 발생 여부를 확인하는 인증 과정을 거친다. 이때, 어떤 키 교환 기술을 사용했는지에 따라 적용할 수 있는 인증방법이 조금씩 다르다[4].

3) 특정 키 배포

3단계는 향후 연결을 위하여 서로의 ID를 확인할 수 있는 key-set을 생성하는 과정으로 앞선 단계와 달리 필수적인 단계는 아니다.

(그림 1)은 위에서 설명한 블루투스 페어링 과정을 그림으로 나타낸 것이다.



(그림 1) Bluetooth Pairing 과정.

2.2 ECDH

ECDH는 타원 곡선 암호화 방식(Elliptic Curve Cryptography, ECC)을 적용한 디피-헬먼 공개키 교환 알고리즘이다. 보안기능을 제공하지 않는 공개된 채널에서 비밀키를 공유하고자 할 때 주로 사용된다[5]. 블루투스에서 ECDH는 키 생성 및 교환 과정에 이용된다.

2.3. 격자 기반 양자 내성 암호

양자 내성 암호는 수학적 문제 기반에 따라 격자(Lattic), 코드(Code), 아이소제니(Isogeny), 다변수(Multivariate), 해시(Hash) 기반 암호로 나뉜다. 이 중 격자 기반 양자 내성 암호는 RSA, ECDH와 같은 공개키 암호 알고리즘을 대체하기 위한 암호 알고리즘이다. 격자를 이용한 난제로 LWE(Learning With Errors) 문제와 SIS(Small Integer Solution) 문제가 주로 이용된다. LWE 문제를 기반으로 한 대표적인 암호 시스템으로는 키 교환 프로토콜 NewHope와 서명 알고리즘 BLISS가 있다.

1) KEM

KEM(Key Encapsulation Mechanism)은 공개키 기반 방식으로 주어진 공개키로 임의의 키를 생성한 후, 생성된 임의의 키를 암·복호화하는 방식을 제공하는 기법이다[10].

KEM의 키 교환 과정은 다음과 같다. Alice가 공

개키와 비밀키를 생성하여 Bob에게 전송하면 Bob은 전달받은 공개키로 임의의 값을 캡슐화(Encapsulation)하여 공유키와 암호문을 생성한다. 이후 Bob은 생성한 암호문을 다시 Alice에게 전송한다. Alice가 전달받은 암호문을 비밀키로 역캡슐화(Decapsulation)하면 Alice는 공유키를 갖게 된다. 두 사람이 동일한 키를 공유하게 되는 것이다[11].

2) NewHope

NewHope는 2016년 Alkim 등에 의해 제안된 DH(Diffie-Hellman)스타일의 알고리즘이다. RLWE (Ring Learning With Errors) 기반의 키 교환 프로토콜로 격자 기반 양자 내성 암호 알고리즘에 속한다[6]. NewHope는 에러 샘플링 알고리즘으로 이항 분포가 적용됐기 때문에 가우시안 분포를 적용한 알고리즘보다 타이밍 공격에 더 안전하다는 장점을 갖는다[7]. 또한, 양자 내성 암호 중 우수한 키 사이즈와 연산 속도를 보인다[8]. 이러한 NewHope는 구글의 브라우저인 크롬 카나리아(Chrome Canary)에 탑재되어 사용된 바 있다[9].

3. 제안기법

본 논문에서 제안하는 기법은 블루투스 페어링 절차 중 2단계 키 생성 및 교환과정과 관련된 것으로, ECDH가 적용되어 있던 부분에 NewHope 알고리즘을 적용하는 것이다. NewHope 기반인 KEM으론 NewHope-CPA-KEM과 NewHope-CCA-KEM이 있는데[10], CPA가 성능 대비 속도가 CCA보다 더 빠르기 때문에 NewHope-CPA-KEM을 선택하였다[12].

제안 기법에 적용된 KEM은 크게 키 생성, 캡슐화, 역캡슐화까지 3단계로 나눌 수 있다.

1) 키 생성

Initiator가 먼저 GEN() 함수를 사용하여 공개키 PK(Public key)와 비밀키 SK(Secret key)를 생성하고, 이 중 공개키만 Responder에게 전송한다.

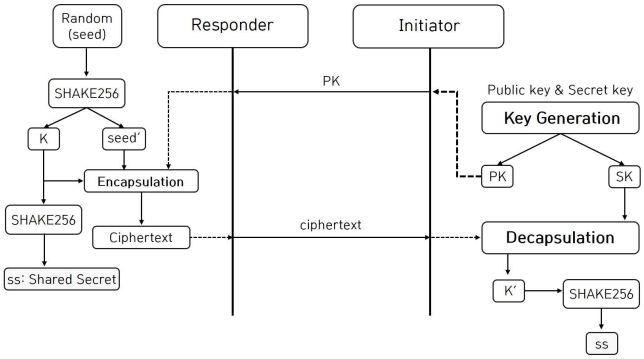
2) 키 캡슐화

PK를 전송받은 Responder는 $\{0, \cdots, 255 RIGHT$ 범위에서 임의의 값을 뽑아 seed에 저장한다. 이후 해시 함수 SHAKE256()에 seed를 입력으로 넣으면 키 K와 seed′가 나온다. seed′와 K, PK를 ENCRYPT() 함수의 입력으로 넣으면 키가 캡슐화되면서 암호문이 생성된다. Responder는 생성된 암호문을 다시 Initiator에게 전송한다.

3) 키 역캡슐화

전달받은 암호문과 개인키 SK를 DECRYPT() 함수를 이용하여 함께 역캡슐화하면 Initiator가 가지고 있던 K′가 Responder에게도 생긴다. 이후, 두 기기가 가지고 있는 K와 K′가 같은지 확인하기 위하여 각각 SHAKE256에 넣은 결과를 비교한다. 두 결괏값이 같다면 두 기기가 동일한 공유키를 가졌다고 볼 수 있다.

(그림 2)는 Initiator와 Responder의 페어링 과정에 적용한 NewHope-CPA-KEM을 도식화 한 것이고, 표 1은 NewHope-CPA-KEM 알고리즘의 공개키와 비밀키, 암호문의 크기를 정리한 것이다.



(그림 2) NewHope-CPA-KEM을 적용한 키 교환 구조

<표 1> NewHope-CPA-KEM 알고리즘의 키 크기와 암호문 크기 (단위 : byte)

Algorithm	PK	SK	Ciphertext
NewHope512-CPA-KEM	928	869	1088
NewHope1024-CPA-KEM	1824	1792	2178

4. 결론

블루투스의 취약점이 발견되었다 하더라도 일상생활에 큰 지장이 있지 않기 때문에 대수롭지 않게 여기고 지나갈 수 있다. 그러나 일상생활과 밀접해지는 만큼 민감한 개인정보가 오가는 경우도 갈수록 늘고 있다. 취약점으로 인해 발생하는 보안 사고를 미연에 방지하기 위해선 블루투스 보안에도 신경을 써야 한다.

본 논문에서는 블루투스의 연결방법과 ECDH, 격자 기반 양자 내성 암호 NewHope에 대해 알아본 후, 블루투스 페어링 단계에 양자 내성 암호를 적용

하는 모델을 제안하였다. 양자 컴퓨터 환경에서 더 이상 안전하지 않다고 판단된 ECDH를 블루투스 페어링 키 교환 단계에서 계속해서 사용한다는 것은 장기적으로 보았을 때 심각한 취약점으로 작용할 수 있다. ECDH 대신 격자 기반 양자 내성 키 교환 프로토콜 중 하나인 NewHope-CPA-KEM을 사용한다면 발생될 것으로 예상되는 취약점을 미리 막을 수 있을 것이다.

5. Acknowledgment

이 논문은 부분적으로 2021년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임(No.2018-0-00264, IoT 융합형 블록체인 플랫폼 보안 원천 기술 연구, 50%) 그리고 부분적으로 2021년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. NRF-2020R1F1A1048478, 25%) 그리고 부분적으로 2021년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (No.2021-0-00540, GPU/ASIC 기반 암호알고리즘 고속화 설계 및 구현 기술개발, 25%).

참고문헌

[1] 최진구, 이재호 “블루투스 표준 기술” 한국통신학회지(정보와통신) 38, 7 (2021) : 75-82.

[2] 양선웅. “자동차 보안 취약점을 이용한 해킹예방과 대응방안” 한국정보기술학회 종합학술발표논문집 , (2017) : 243-246.

[3] Claverie, Tristan & Esteves, José “BlueMirror: Reflections on Bluetooth Pairing and Provisioning Protocols.”, 2021 IEEE Security and Privacy Workshops(SPW), (2021) : 339-351.

[4] 이재령, 최원석, 이동훈 “블루투스 Passkey Entry 인증 모드에 대한 MITM 공격과 대응방법” 정보처리학회논문지. 컴퓨터 및 통신시스템 5, 12 (2016) : 481-490.

[4] 신설희, 김은기 “MPTCP에서 ECDH를 이용한 세션 키 자동생성에 관한 연구” 한국정보통신학회논문지 20, 10 (2016) : 1912-1918.

[6] 이주엽, 김수리, 김창한, 홍석희 “μ-Hope : 오류정정 부호를 사용한 RLWE 기반의 경량 KEM.” 정보보호학회논문지 30.5 (2020): 781-793.

[7] 최락용, 안형철, 이지은, 김성숙, 김광조 “양자 컴퓨터 공격에 안전한 격자 기반 키 교환 방식의 비교” 한국통신학회논문지 42, 11 (2017) : 2200-2207.

[8] 백주연, 김동규 “Lattice 기반 양자 암호 알고리즘의 하드웨어 최신 구현 동향” 대한전자공학회 학술대회, (2020) : 562-566.

[9] 김수리, 김한빛, 김희석. “격자 기반 차세대 양자내성 암호에 대한 부채널 분석 기술 동향” 정보보호학회지 27, 6 (2017) : 33-40.

[10] 박제홍, 권대성 “Key Encapsulation Mechanism” 정보보호학회지 14, 5 (2004) : 44-49.

[11] 박찬희, 윤영여, 박해룡, 최은영, 김호원 "격자기반 양자내성 키 교환 알고리즘 구현" 정보보호학회지 30, 3 (2020) : 11-16.

[12] E. Alkim, et al., “NewHope: Algorithm specification and supporting documentation,” Submission to the NIST Post-Quantum Cryptography Standardization Project (2019)