정 보 보 호 학 회 지
제 31 권 제2호, 2021. 4

양자컴퓨터 상에서의 양자 알고리즘의 위협과 양자 내성을 가지는 양자 내성 암호에 대한 최신 연구 동향

장 경 배*, 김 현 지*, 송 경 주*, 서 화 정**

요 약

본 고에서는 정보보호학회 젊은 연구자 30인으로 선정된 한성대학교 서화정 교수의 주요 연구 분야에 대해 확인해 본다. 특히 서화정 교수가 집중하고 있는 연구 분야인 양자컴퓨터와 양자내성암호 그리고 이와 관련된 저명한 국제 학회인 PQCrypto와 CHES의 최신 동향에 대해 확인해 본다.

Ⅰ. 서 론

서화정 교수는 2017년에 한성대학교 사이버 보안 트랙에 임용되어 현재는 사이버 보안 트랙 주임 교수로써 근무하고 있다. 한성대학교 사이버 보안 트랙은 총 4분의 교수님에 의해 운영되고 있다. 특히 네트워크 보안을 담당하고 계신 김승천 교수님, 암호학을 담당하고 계신 이후진 교수님, 자동차 보안을 담당하고 계신 최원석 교수님, 그리고 보안 응용을 담당하고 계신 서화정 교수님으로 구성되어 있다. 한성대학교의 경우 두 개의 트랙을 선택하는 복수 전공을 모든 학생에게 적용하고 있으며 많은 사이버보안 트랙 학생들이 사물인터넷 트랙과의 연계를 통해 사물인터넷 보안을 학습하고 있다.

서화정 교수가 운영하고 있는 암호 구현 연구실 (https://crypto.modoo.at/)에서는 최근에 암호학계에서 큰 관심을 받고 있는 양자컴퓨터와 양자내성암호에 대해 연구실 소속 대학원생들과 함께 연구하고 있다. 작년에 연구실에서 수행한 괄목할만한 성과로는 국산 암호(LEA, CHAM, 그리고 HIGHT)에 대한 양자컴퓨터 구현을 국내 최초로 수행했다는 점과 NIST 양자 내성 암호 공모전 3 라운드에서 대체 양자 내성 암호군으로 분류된 SIKE를 pqm4 라이브러리에 추가하였다는 것이다 [1,2].

본 고에서는 서화정 교수가 집중하고 있는 연구 분야인 양자컴퓨터와 양자내성암호 그리고 이와 관련된 최신 학회 동향에 대해 확인해 보며 구성은 아래와 같다. 2장에서는 양자컴퓨터와 보안 이슈에 대해 확인해 본다. 3장에서는 양자내성암호와 NIST 양자 내성 암호 공모전에 대해 확인해 본다. 4장에서는 양자컴퓨터와 양자내성암호와 관련 학회인 PQCrypto (https://pqcrypto2020.inria.fr/)와 CHES (https://ches.iacr.org/index.php)의 최신 연구 동향에 대해 확인해 본다. 5장에서는 본고를 마무리한다.

Ⅱ. 양자 컴퓨터와 보안 이슈

2.1. 양자 컴퓨터의 개발

양자 컴퓨터는 비트가 아닌 큐비트를 사용하여 기존 비트 위주 컴퓨터에서는 불가능했던 양자 알고리즘을 실행하는 것이 가능하다. 현재 구글, IBM, 그리고 Honeywell에서는 양자 컴퓨터 개발에 적극적으로 참여하고 있다. 양자 컴퓨터 개발에 있어 주요 과제는 큐비트의 정보를 제어 및 관찰하면서, 다른 환경으로부터 완전히 격리시키는 것이다. 특히 오류율을 최소화하기 위해, 양자 컴퓨터 시스템은 액체 헬륨을 사용하여 매우 낮은 온도에서 실행된다. 양자 컴퓨터 개발에는 대표적으로 2가지 방식이 존재한다. IBM과 구글에서는 초전

본 연구는 2021년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. NRF-2020R1F1A1048478).
* 한성대학교 IT융합공학부 (대학원생, starj1023@gmail.com: 대학원생, khj1594012@gmail.com: 대학원생, thdrudwn98@gmail.com)
** 한성대학교 IT융합공학부 (조교수, hwajeong84@gmail.com)

도 큐비트를 구현하는 방식을 사용하며 Honeywell에서는 이온트랩 큐비트를 구현하는 방식을 사용하고 있다.

양자 컴퓨터의 성능척도를 평가하는 대표적인 지표 중 하나는 큐비트 수이다. 하지만 단순히 큐비트 수만을 가지고 성능을 평가하기에는 한계점이 존재하기에 다른 요소들을 함께 고려한다. 이 중에서 대표적인 수치가 바로 큐비트 연결성이다. 양자 컴퓨터의 큐비트들이 서로 얼마나 많이 연결되어 있는지를 의미하며 큐비트를 늘릴수록 어렵다. 추가적으로 IBM에서는 양자컴퓨팅의 실실적인 수행능력을 측정하기 위해 양자 볼륨(Quantum Volume) 이라는 새로운 척도를 도입하였다. 양자 볼륨은 회로 연결, 큐비트의 수와 품질, 그리고 오류발생빈도의 수치를 종합한 실직적인 양자 컴퓨팅 수치를 나타낸다.

2.2. 보안 이슈

양자컴퓨터의 높은 연산량은 인공지능과 시뮬레이션과 같은 분야에서 활발히 활용될 것으로 보인다. 하지만 양자컴퓨터의 발달은 현대 암호화 시스템의 붕괴를 가속화시키는 부정적인 측면도 함께 가지고 있다. 암호화 알고리즘은 보안통신 상에 필요한 기밀성, 무결성, 그리고 인증을 만족하기 위해 사용되고 있다. 하지만 양자컴퓨터의 시대가 다가옴에 따라 암호화 알고리즘은 큰 위기에 직면해 있다. 대표적으로 Shor 알고리즘과 Grover 알고리즘이 있다[3, 4]. 공개키 암호화에 널리 사용되고 있는 RSA와 ECC 알고리즘의 안전성은 소인수분해와 이산대수 문제에 기반한다. 그러나 Shor 알고리즘은 이러한 문제를 다항 시간 안에 풀어낼 수 있다. 최근 PQCrypto‘20 그리고 CHES’20 에서는 공개키 암호화 알고리즘인 ECC (Elliptic Curve Cryptography)의 이산대수 문제에서 가장 많은 비용을 차지하는 타원곡선 스칼라 곱셈을 양자 회로 상에서 구현한 논문이 발표되었다 [5, 6]. 해당 연구에서는 공격에 필요한 큐비트 수를 최소화 하는데 초점을 두었으며 실제 양자컴퓨터로 공격할 때 ECC가 RSA보다 더 취약함을 보였다. 특히 RSA-2048를 인수분해 하기 위한 Shor 알고리즘은 약 4,000개 이상의 안정적인 큐비트 그리고 수십억 개의 양자 게이트가 필요하다. 여기서 약 4,000개 이상의 큐비트는 오류가 전혀 발생하지 않는 안정적인 큐비트를 가정한다. 하지만 오류가 전혀 발생하지 않는 큐비트는 현실적으로 불가능하다. 하나의 안정적인 큐비트를 구현하기 위해서는 오류정정을 위한 100개의 추가적인 큐비트가 필요하다. 현재 양자 컴퓨터의 발달 과정과 실질적인 오류 제어 능력을 고려해본다면, 약 40만개 이상의 큐비트를 가진 양자 컴퓨터가 개발되었을 때, 안정적인 4,000개의 큐비트로 Shor 알고리즘을 동작시키는 것이 가능하다. 현 시점에서는 양자컴퓨터를 통한 실질적인 공격이 먼 미래의 이야기이지만 양자컴퓨터 상에서의 양자 알고리즘을 통한 공격에 대비하여 현재 사용되고 있는 취약한 암호화 알고리즘을 사전에 교체하는 작업이 필요하다. 이러한 암호를 양자 컴퓨터로도 풀기 어려운 수학적 난제들에 기반한 양자 내성 암호라고 하며 미국의 NIST에서 표준화 작업을 진행중에 있다[7].

반면에 대칭키 분야에서는 공개키 만큼의 보안 취약점이 발견되고 있지는 않다. 다만 Grover 알고리즘은 대칭키 암호 알고리즘의 n-비트 안전성을 n/2-비트로 감소시킨다. 다시 말하면 현재 암호화 알고리즘으로 128-비트 AES를 사용하고 있다면, 키 길이를 2배 늘린 256-비트 AES를 통해 보안성을 확보할 수 있다.

위에서 살펴본 양자 컴퓨터상에서의 양자 알고리즘의 적용은 최근 6,000만원을 돌파하며 큰 관심을 받고 있는 비트코인의 안전성에 큰 취약점을 발생시키게 된다. 비트코인에서는 ECC를 통해 개인키와 공개키를 생성하고 ECDSA (Elliptic Curve Digital Signature Algorithm)와 생성된 개인키를 통해 발생한 트랜잭션에 대한 전자서명을 수행한다. 만약 양자컴퓨터를 사용하여 해당 암호화폐에 사용되는 개인키를 해킹한다면 사용자들의 지갑에 대한 접근이 가능하며 이는 블록체인 시스템의 파괴로 이어진다. 이와 더불어 Grover 알고리즘을 통해 작업 증명에 사용되는 해시 함수에 대한 해킹 또한 가능하다. 따라서 최근에는 이러한 위협에 대비하고자 양자 내성을 가진 암호 화폐인 QRL (Quantum Resistant Ledger)이 개발되고 있다.

Ⅲ. 양자내성 암호와 NIST 양자 내성 암호 공모전

NIST에서는 현재 양자내성암호 표준화 작업을 진행하고 있으며 빠르면 2년 내에 1차 최종 양자 내성 암호 알고리즘을 선정하여 발표할 예정이다. 상세한 NIST 양자 내성 암호 표준화 일정은 [표 1]과 같다.

〔표 1〕 NIST 양자 내성 암호 표준화 일정

기존 일정	수정된 일정	내용
2017. 11	2017. 11	알고리즘 제안 마감
2018. 04	2018. 04	제안 알고리즘 소개
2018~2019	2018~2019	1차 평가분석 진행 (1차 후보 선정)
2019. 08	2019. 01	1차 선정 결과 발표
2020~2021	2019~2020	2차 평가분석 진행 (2차 후보 선정)
2022~	2020. 07	2차 선정 결과 발표
	2020~2022	3차 평가분석 진행 (최종 후보 선정)
	2022~2024	최종 선정 결과 발표 및 표준화

공개키 암호 (RSA 그리고 ECC)에서 가장 중요한 기능은 키 교환과 전자 서명이다. 하지만 양자 내성 암호 후보 알고리즘들은 하나 이상의 문제점을 지니고 있다. 예를 들어 서명 혹은 키 크기가 너무 크다거나 과도한 연산이 필요한 경우이다. 현재 PQCrypto와 CHES 등과 같은 저명한 국제 학회에서는 NIST 양자내성암호 후보 알고리즘에 대한 최적화 구현 기법이 발표되고 있다. 이와 더불어 양자내성암호 알고리즘 중에서는 계산 결과에 불확실성이 포함되는 경우에는 공개키 유효성과 복호화 실패에 대한 해결책을 반드시 제공해야 한다. 현재 NIST 공모전에서 양자내성암호 알고리즘의 평가기준은 보안 안전성과 연산 성능에 중점을 두고 있다. 안전성 측면에서는 양자 컴퓨터와 기존 컴퓨터의 공격으로부터도 안전성을 확보할 수 있어야 하며 성능 측면에서는 다양한 플랫폼 상에서의 고속 구현이 보장되어야 한다. 이와 더불어 기존 프로토콜 및 네트워크와의 호환성을 보장해서 drop-in 형식으로 새로운 알고리즘 적용이 가능해야 하며 보안성 측면에서는 perfect forward secrecy를 달성해야 한다. 또한 부채널 공격에 대한 내성과 더불어 알고리즘은 간단하고 유연성을 충분히 만족해야 한다. 현재 NIST에서는 양자 내성 암호 2차 선정 결과를 발표한 상황이며 이에 대한 상세한 내용은 [표 2]와 같다.

하지만 양자 내성 암호의 실질적인 보안 안전성에 대한 분석에는 어려움이 있다. 기존 컴퓨터 상에서의 공격에 대한 안전성은 현재 많은 연구가 진행되어 분석이 가능하지만 양자 알고리즘을 사용한 공격에 대해서는 여전히 불확실성이 존재한다. 이는 양자 컴퓨터가 개발

〔표 2〕 NIST 양자 내성 암호 2차 선정 결과

종류	구분	Finalist	Alternate	장점	단점
격자 기반	암호화/키교환	CRYSTALS-KYBER, NTRU, SABER	FrodoKEM, NTRU Prime	빠른 연산 속도	파라미터 설정 어려움
	전자서명	CRYSTALS-DILITHIUM, FALCON	-		
다변수 다항식 기반	암호화/키교환	-	-	작은 서명 크기와 빠른 연산 속도	큰 키 사이즈
	전자서명	Rainbow	GeMSS		
해시 기반	암호화/키교환	-	-	안전성 증명 가능	큰 서명 사이즈
	전자서명	-	SPHINCS+		
아이소지니 기반	암호화/키교환	-	SIKE	작은 키 사이즈	느린 연산속도
	전자서명	-	-		
코드 기반	암호화/키교환	Classic McEliece	BIKE, HQC	빠른 암호화 및 복호화 속도	큰 키 사이즈
	전자서명	-	-		
영지식 기반	암호화/키교환	-	-	number-theoretic 혹은 structured hardness에 기반하지 않음	큰 서명 사이즈
	전자서명	-	Picnic		

되기 이전에는 실제 공격을 수행해 볼 수 없을 뿐 아니라 새로운 양자 알고리즘의 등장으로 공격 기법이 개선될 가능성 또한 존재함을 의미한다. 이러한 불확실성으로 인해 양자내성암호 표준화 공모전은 기존에 수행되었던 AES 그리고 SHA 공모전보다 최종 후보 선정에 있어 어려움이 많을 것으로 보인다. 현재 양자내성암호 후보군 중 완벽한 알고리즘은 존재하지 않으며 각자 하나 이상의 단점을 가지고 있다. 따라서 알고리즘 간의 단점을 보완하기 위해 하나의 알고리즘이 아닌 다수의 우수한 알고리즘들이 표준화될 것으로 예상되고 있다. NIST의 최종 표준안이 결정되면 기존 암호시스템을 양

자 내성 암호 시스템으로의 전환이 본격화될 것이다.

Ⅳ. 양자 컴퓨터 및 양자 내성 암호 관련 학회

본 장에서는 양자 컴퓨터 도래로 인해 큰 관심을 받고 있는 양자내성암호 국제 학술대회 (PQCrypto)와 전통적인 암호 구현 최적화 국제 학술대회 (CHES)에 대해 확인해 본다.

4.1. PQCrypto 최신 동향

PQCrypto는 2006년을 시작으로 매년 개최되는 양자 컴퓨터와 관련된 국제 학술대회이다. 양자 내성암호를 전문적으로 다루는 학술대회인 만큼 가장 최신의 양자 내성암호 연구결과가 발표되고 있다. 아래에서는 최근 PQCrypto에서 발표된 연구 동향 중 암호 구현 부분에 집중하여 기술하도록 한다.

양자 내성 암호는 실제 네트워크 보안 프로토콜인 TLS로의 drop-in 형식으로의 적용이 중요하다. Paquin et. al.은 Linux 커널의 네트워킹 기능을 사용하여 다양한 네트워크 조건 상에서 양자 내성 암호를 활용한 하이브리드 TLS 프로토콜의 핸드셰이크 성능을 측정 및 분석하였다[8].

최종 후보군으로 선정된 양자 내성 암호 프리미티브 중 다변수 다항식 기반 양자 내성 암호 Rainbow는 작은 서명 크기와 빠른 연산 속도로 큰 관심을 받고 있다 [9]. Petzoldt는 Rainbow의 느린 키 생성 알고리즘을 최대 2 배까지 가속화하는 알고리즘을 제안하였다. 이와 더불어 Cyclic Rainbow 서명 알고리즘에 대한 개선된 키 생성 알고리즘을 제안하였다. 개선된 알고리즘을 사용하면 표준 Rainbow의 키 쌍과 동일한 시간에 Cyclic Rainbow에 대한 키 쌍을 생성할 수 있다. 이를 통해 Cyclic Rainbow를 표준화 알고리즘에 적용할 수 있는 실용적인 방안을 제시하였다.

격자 기반 양자 내성 암호 구현에 있어 정수 가우스 샘플링의 안전하고 효율적인 구현은 중요하다 [10]. Howe et. al.은 이산 가우스를 생성을 위한 모듈식 프레임워크를 제안하였다. 해당 프레임워크는 간단하며 보안성 입증이 가능할 뿐 아니라 타이밍 공격에 대한 내성도 가진다. 해당 샘플러는 최근 Falcon 서명체계에도 적용되었다.

QC-MDPC를 사용하는 코드기반 키 교환 메커니즘은 quasi-cyclic syndrome decoding과 quasi-cyclic codeword finding과 같은 코딩이론의 가정하에 IND-CPA 보안을 달성할 수 있다. 더 높은 보안 요구사항을 달성하기 위해서는 디코딩 알고리즘과 적절한 매개변수 선택을 통해 무시할 수 있는 디코딩 실패율 (DFR)을 증명하는 것이 필요하다. Sendrier는 디코더에 대한 추가적인 보안 가정 하에서 낮은 DFR을 보장하는 새로운 디코더 Backflip을 제안하였다 [11].

Ring-LWE를 기반으로 하는 키교환 프로토콜인 NewHope은 NIST 양자 내성 암호 공모전 후보군에는 선정되지 못하였지만 큰 관심을 받고 있는 알고리즘이다. Amiet et. al.은 Cortex-M4 프로세서 상에서 실행되는 NIST 공모전의 참조구현물을 타겟으로 하여 공유된 비밀키에 대한 새로운 부채널 공격 메커니즘을 보였다 [12]. 특히 전력측정을 기반으로 하여 하나의 단일 파형 데이터에서 완전한 비밀키를 추출하였다. 이와 더불어 컴파일러 최적화 옵션에 따른 전력 소비 패턴을 분석하여 공격하였다. 최적화 옵션을 -O0으로 한 경우 비밀키를 오실로스코프상에서 육안으로 직접 확인할 수 있다. 최적화가 활성화된 경우에는 DPA (Differential Power Analysis)와 같은 분석 기술을 통해 단일 전력 파형을 통해 공격 가능함을 보였다.

4.2. CHES 최신 동향

세계 암호 학회 IACR의 지역 컨퍼런스인 CHES (Conference on Cryptographic Hardware and Embedded Systems)에서는 암호화 하드웨어 및 소프트웨어 구현의 설계 및 분석에 대한 최신 연구 결과를 발표한다. 1999년 미국을 시작으로 연례 컨퍼런스를 진행해 왔으며 2014년에는 한국의 부산에서도 개최되었다. CHES는 2020년도에 중국 베이징에서 열릴 예정이었으나 코로나 상황으로 인해 온라인으로 비대면 행사로 진행되었다. 따라서 2021년도에 CHES는 중국 베이징에서 개최될 예정이다. 암호 구현의 최신 결과를 다루는 학회인 만큼 최근 CHES에서는 양자 내성 암호 최신 구현을 다루고 있다. 아래에서는 CHES에 발표된 최신 양자 내성 암호 구현 관련 연구 동향에 대해 기술 한다.

격자기반 전자서명 기법인 Dilithium은 최종 후보군으로 선정된 만큼 그 관심도가 높아지고 있다.

Greconici et. al.은 ARM Cortex-M3와 ARM Cortex-M4 상에서의 NTT와 Inverse NTT 연산을 20% 이상 향상시켰다 [13]. 이와 더불어 Cortex-M3 상에서 Constant timing으로 연산이 가능한 결과를 최초로 제시하였다.

또 다른 격자 기반 양자 내성 암호인 NTRU Prime의 경우 polynomial ring에 기반하고 있으며 NTT을 통한 연산 가속화가 용이하지 못하다. Alkim et. al.은 Good의 트릭과 mixed radix NTT를 통해 기존 Toom-Cook 기반 polynomial multiplication을 ARM Cortex-M4 상에서 32% 그리고 17% 향상시킨 결과를 도출하였다 [14]. 특히 ntrulpr761 파라미터의 경우 9~16% 연산 성능을 향상시켰으며 15~39%의 메모리 사용량을 감소시켰다.

해시 기반 서명 알고리즘 중 XMSS 서명 알고리즘은 IETF RFC 8391 표준화가 진행되었다. XMSS 알고리즘에 대한 서명 고속 검증 기법을 통해 연산 성능을 향상시키는 방법을 Bos et. al.이 제안하였다 [15]. 일반 컴퓨터 상에서 서명 시간을 약 1.44배 향상시켰으며 ARM Cortex-M4 상에서 최적화 구현 결과를 제시하였다.

현재 연구가 활발히 진행되고 있는 구현 플랫폼으로는 ARM Cortex-M4와 Artix FPGA가 있다. 이와 더불어 유연한 명령어셋 확장이 가능한 RISC-V 상에서의 양자 내성 암호 구현이 활발히 연구되고 있다. RISC-V 상에 양자 내성 암호를 위한 명령어 셋을 추가하여 격자기반 암호를 향상시킨 RISQ-V가 Fritzmann et. al.에 의해 제안되었다 [16]. RISQ-V는 리소스 재사용과 메모리 접근을 줄였으며 연산 성능을 크게 향상시켰다.

V. 결 론

본 고에서는 정보보호학회 젊은 연구자 30인으로 선정된 한성대학교 서화정 교수의 주요 연구 분야인 양자컴퓨터와 양자내성암호에 대해 확인해 보았다. 앞으로 해당 연구 분야는 암호학계에 있어 큰 영향력을 미칠 것으로 예상된다. 따라서 선제적으로 양자 내성 암호로의 전환을 사회 전반 인프라에 걸쳐서 고려해야 할 것이다. 이와 더불어 양자컴퓨터와 양자내성암호에 대한 연구와 개발이 산학연에서 보다 활발히 수행되어야 할 것이다.

참 고 문 헌

[1] K. Jang, S. Choi, H. Kwon, H. Kim, J. Park, H. Seo, “Grover on Korean Block Ciphers,” Applied Sciences, 10(18), 6407, 2020.

[2] H. Seo, M. Anastasova, A. Jalali, R. Azarderakhsh, “Supersingular isogeny key encapsulation (SIKE) round 2 on ARM Cortex-M4,” IEEE Transactions on Computers, 2020.

[3] P. W. Shor, “Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer,” SIAM review, 41(2), pp. 303-332, 1999.

[4] L. K. Grover, “A fast quantum mechanical algorithm for database search,” In Proceedings of the twenty- eighth annual ACM symposium on Theory of computing, pp. 212-219, 1996.

[5] T. Häner, S. Jaques, M. Naehrig, M. Roetteler, M. Soeken, “Improved quantum circuits for elliptic curve discrete logarithms,” In International Conference on Post-Quantum Cryptography, pp. 425-444, 2020.

[6] G. Banegas, D. J. Bernstein, I. van Hoof, T. Lange, “Concrete quantum cryptanalysis of binary elliptic curves,”“ IACR Transactions on Cryptographic Hardware and Embedded Systems, pp. 451-472, 2021.

[7] W. Barker, W. Polk, M. Souppaya, ”Getting Ready for Post-Quantum Cryptography: Explore Challenges Associated with Adoption and Use of Post-Quantum Cryptographic Algorithms,“ National Institute of Standards and Technology, 2020.

[8] C. Paquin, D. Stebila, G. Tamvada, ”Benchmarking post-quantum cryptography in TLS,” In International Conference on Post-Quantum Cryptography, pp. 72-91, 2020.

[9] A. Petzoldt, “Efficient key generation for rainbow,” In International Conference on Post-Quantum Cryptography, pp. 92-107, 2020.

[10] J. Howe, T. Prest, T. Ricosset, M. Rossi, “Isochronous Gaussian sampling: from inception

to implementation," In International Conference on Post-Quantum Cryptography, pp. 53-71, 2020.
[11] N. Sendrier, V. Vasseur, "About low DFR for QC-MDPC decoding," In International Conference on Post-Quantum Cryptography, pp. 20-34, 2020.
[12] D. Amiet, A. Curiger, L. Leuenberger, P. Zbinden, "Defeating NewHope with a single trace," In International Conference on Post-Quantum Cryptography, pp. 189-205, 2020.
[13] D. O. Greconici, M. J. Kannwischer, D. Sprenkels, "Compact Dilithium Implementations on Cortex-M3 and Cortex-M4," IACR Transactions on Cryptographic Hardware and Embedded Systems, pp. 1-24, 2021.
[14] E. Alkim, D. Y. L. Cheng, C. M. M. Chung, H. Evkan, L. W. L. Huang, V. Hwang, B. Y. Yang, "Polynomial Multiplication in NTRU Prime," IACR Transactions on Cryptographic Hardware and Embedded Systems, pp. 217-238, 2021.
[15] J. W. Bos, A. Hülsing, J. Renes, C. van Vredendaal, "Rapidly Verifiable XMSS Signatures," IACR Transactions on Cryptographic Hardware and Embedded Systems, pp. 137-168, 2021.
[16] T. Fritzmann, G. Sigl, J. Sepúlveda, "RISQ-V: Tightly coupled RISC-V accelerators for post-quantum cryptography," IACR Transactions on Cryptographic Hardware and Embedded Systems, pp. 239-280, 2020.

〈저 자 소 개〉

장 경 배 (Kyungbae Jang)
학생회원
2019년 2월 : 한성대학교 IT응용시스템공학과 공학 학사
2021년 2월 : 한성대학교 IT융합공학과 석사과정
2021년 3월~현재 : 한성대학교 IT융합공학과 박사과정
<관심분야> 양자 컴퓨터, 정보보안

김 현 지 (Hyunji Kim)
학생회원
2020년 2월 : 한성대학교 IT응용시스템 공학 학사
2020년 3월~현재 : 한성대학교 IT융합공학과 석사과정
<관심분야> 정보보안, 인공지능

송 경 주 (Gyeongju Song)
학생회원
2021년 2월 : 한성대학교 IT응용시스템공학과 공학 학사
<관심분야> 양자 컴퓨터, 정보보안

서 화 정 (Hwajeong Seo)
종신회원
2010년 2월 : 부산대학교 컴퓨터공학과 학사
2012년 2월 : 부산대학교 컴퓨터공학과 석사
2016년 1월 : 부산대학교 컴퓨터공학과 박사
2016년 1월~2017년 3월 : 싱가포르 과학기술청
2017년 4월~현재 : 한성대학교 IT 융합공학부 조교수
<관심분야> 암호구현