DBpia

논문 19-44-07-01 The Journal of Korean Institute of Communications and Information Sciences '19-07 Vol.44 No.07
https://doi.org/10.7840/kics.2019.44.7.1239

양자내성암호 하드웨어 구현 동향 및 분석

박 찬 희◆, 김 해 용*, 지 장 현*, 김 호 원°

A Survey on Post-Quantum Cryptography Hardware Implementation Trends and Analysis

Chan-hui Park◆, Hae-young Kim*, Jang-hyun Ji*, Ho-won Kim°

요 약

최근 양자 컴퓨팅 기술 발전에 따라 Grover 알고리즈 및 Shor 알고리즘과 같은 양자 컴퓨팅 알고리즘에 의해 기존에 사용되고 있는 대칭키 및 공개키 암호의 보안 취약점이 발생한다. 2011년 양자어닐링 기법을 적용한 최초의 128큐비트 양자컴퓨터가 개발된 이후 점차 진보한 양자컴퓨터가 개발되고 있다. 이에 따라 양자컴퓨팅 시대에 대비하여 안전하고 신뢰할 수 있는 양자내성암호(Post-Quantum Cryptography)에 대한 연구가 진행되고 있으며, 미국 NIST에서는 양자내성암호 표준 공모전을 진행하고 있다. 2017년 11월 82종의 양자내성암호가 제출되었으며, 현재 1차 평가가 종료된 후 26종의 암호 알고리즘이 후보로 선정되었다. 향후 내부 평가를 거쳐 약 4종의 표준 알고리즘을 선정할 것으로 기대하고 있다. 현재 양자내성암호 표준 공모전에서는 소프트웨어 구현물에 대한 평가만 진행이 되고 있으며, 효율적인 하드웨어 구현을 위한 다양한 연구도 진행되고 있다. 따라서, 본 논문에서는 양자내성암호 하드웨어 구현 결과물에 대한 동향 및 성능 평가 결과를 비교 분석하고 향후 연구 방향에 대해 기술하고자 한다.

Key Words : Post-Quantum Cryptography, Quantum Computer, Hardware Implementation, Field Programmable Gate Array(FPGA)

ABSTRACT

Recent advances in quantum computing technology have led to security vulnerabilities in symmetric keys and public key cryptography that have been used by quantum computing algorithms such as Grover and Shor. Since the first 128 qubit quantum computer with quantum annealing technique developed in 2011, a progressive quantum computer is being developed. As a result, research on safe and reliable Post Quantum Cryptography is underway in preparation for the era of quantum computing, and NIST is conducting a competition for standards. In November 2017, 82 kinds of algorithms were submitted, and 26 kinds of algorithms were selected as candidates after the first evaluation. We expect to select about four standard algorithms through internal evaluation. Currently, evaluation of software implementations is underway in the Standards Competition, various research results for effective hardware implementation are being published. In this paper, we compare and analyze trends and performance evaluation results of Post-Quantum cryptography hardware implementations and describe future research direction.

※ 이 논문은 부산대학교 기본연구지원사업(2년)에 의하여 연구되었음

◆ First Author : Pusan National University Department of Computer Science and Engineering, chan70921@pusan.ac.kr, 학생회원
° Corresponding Author : Pusan National University Department of Computer Science and Engineering, howonkim@pusan.ac.kr, 종신회원
* Pusan National University Department of Computer Science and Engineering, {ryoung0327, jjh0819}@gmail.com
논문번호 : 201810-294-A-RE, Received September 30, 2018; Revised March 26, 2019; Accepted May 2, 2019

www.dbpia.co.kr

Ⅰ. 서 론

양자 컴퓨터(Quantum Computer)는 중첩(Superposition)과 얽힘(Entanglement)과 같은 양자적 성질을 이용하여 고속의 연산이 가능하도록 만들어진 특수한 컴퓨터이다. 2011년 D-WAVE Systems Inc.는 양자 어닐링(Quantum Annealing) 기법을 이용하여 세계 최초로 128큐비트 양자컴퓨터를 개발하였으며, 현재 2000큐비트 수준의 양자컴퓨터가 등장하였다. 최근에는 D-Wave Systems Inc.뿐만 아니라 Google, IBM도 양자컴퓨터 개발을 위해 많은 투자를 하고 있다. 이러한 양자 컴퓨팅 기술의 발전에 따라 대표적인 양자 알고리즘인 Grover 알고리즘과 Shor 알고리즘으로 인해 기존 현대암호의 안전성에 위협을 받고 있다.

1996년 Lov Grover에 의해 제안된 Grover 알고리즘[1]은 양자 컴퓨터상에서의 데이터베이스 검색 속도를 향상시킬 수 있는 방법이다. 이는 DES, AES 등 대칭키 알고리즘에 대한 전수 조사 공격(Brute Force Attack)을 통해 비밀키를 알아낼 수 있다. 양자 컴퓨팅 환경에서 안전한 대칭키 암호 알고리즘을 사용하기 위해서는 비밀키의 길이를 현재보다 2배 이상 늘려야 한다. 1994년 Peter Shor에 의해 제안된 Shor 알고리즘[2]은 큰 수에 대한 소인수분해 문제 및 이산대수 문제(Discrete Logarithm)를 다항식 시간 내 공격이 가능하다. 이로 인해 RSA, ECC 등 현존하는 공개키 암호 알고리즘에 대한 공격이 가능하다.

현대암호의 안전성 위협에 따라 미국 국립표준기술연구소(National Institute of Standards and Technology, NIST)는 "Report on Post-Quantum Cryptography[3]"를 통해 양자내성암호(Post-Quantum Cryptography, PQC)의 필요성을 강조하였다. 2016년 2월 PQCrypto 2016에서 양자내성암호 표준 공모전을 발표하였다. 2018년 1차 후보군 69종이 선정되었으며, 내부 평가를 거쳐 17종의 공개키 암호 알고리즘과 9종의 전자 서명 알고리즘이 2차 후보로 선정되었다.

현재 NIST 양자내성암호 표준 공모전에서는 소프트웨어 구현물(C 코드)에 대한 평가를 진행되고 있다. 암호 알고리즘의 소프트웨어 구현의 경우 하드웨어 구현에 비해 저비용으로 구현할 수 있으며 유지보수가 편리하다는 면에서 장점이 있으나, 운영체제(OS)의 보안 취약성으로 인한 안전성문제, 리버스 엔지니어링(Reverse Engineering), 공유메모리 사용 등 다수의 단점이 존재한다. 이러한 단점으로 인해 특정 환경에서는 암호 알고리즘의 하드웨어 구현을 요구하고 있으며, 양자내성암호의 경우에도 하드웨어 구현물의 필요성이 제기되고 있다.

따라서 본 논문에서는 양자내성암호의 유형별 하드웨어 구현 동향에 대해서 살펴보고자 한다. 표준 공모전 이전에도 양자내성암호와 관련된 다양한 연구들이 진행되어 왔으며, 기존 논문 및 표준 공모전 제출물에 대한 하드웨어 최적화 구현 방법, 구현 환경, 그리고 성능 결과에 대해 기술한다.

본 논문의 구성은 다음과 같다. Ⅱ장에서 양자내성암호 표준 공모전 제출물에 대한 종류 및 특성에 대해 기술한다. Ⅲ장에서는 암호 알고리즘별 하드웨어 최적화 구현 및 구현 결과에 대해 비교 분석하며, Ⅳ장에서는 결론 및 향후 연구 방향에 대해 기술한다.

Ⅱ. 양자내성암호 표준 공모전 제출물 종류 및 특성

양자내성암호의 종류는 크게 5종류로 구분되며 각 유형별 특성은 다음과 같다.

1) 격자 기반(Lattice-based) 암호: 1996년 Ajtai가 제안한 격자 기반 양자내성암호[5]는 격자(Lattice)상에서 SVP(Shortest Vector Problem), CVP(Closest Vector Problem)의 어려움에 기반한 암호 알고리즘
2) 코드 기반(Code-based) 암호: 1978년 McEliece에 의해 제안된 코드 기반 암호 알고리즘[11]으로 해밍 코드(Hamming Code)에 대해 임의의 에러 벡터(Random Error Vector)를 주입하고 이 에러 벡터를 구하는 것이 NP-hard 문제임을 기반으로 하는 알고리즘

   다변수 기반(Multivariate-based) 암호: 1988년 Matsumoto, Imai에 의해 제안된 다변수 기반의 양자내성암호[19]는 유한체 상에서 다변수 함수의 해를 구하는 것이 NP-hard 문제임을 기반으로 하는 암호 알고리즘
3) 아이소제니 기반(Isogeny-based) 암호: 2011년 Luca De Feo, Plut Jao에 의해 제안된 아이소제니 기반 양자내성암호[20]는 동일한 차수(Order)를 가지는 두 타원 곡선(Elliptic Curve)상에 존재하는 아이소제니를 구하는 것이 NP-hard 문제임을 기반으로 하는 암호 알고리즘
4) 해시 기반(Hash-based) 암호: 1979년 Ralph Merkle에 의해 제안되었으며 해시 암호의 안전성에 의존하고 있어 안전성 증명이 가능한 암호 알고리즘

www.dbpia.co.kr

NIST에서는 1차 후보군 중 안전성, 성능, 그리고 상기 암호 유형별 특성을 고려하여 2차 후보군을 선정하였다. 2019년 1월 2차 후보군[4]이 발표되었으며, 1차 후보군 69종의 알고리즘 중 26종이 선정되었으며, 각 알고리즘의 종류는 표 1, 2와 같다.

2차 후보군의 선정 결과를 살펴보면 격자 기반(Lattice-based) 12종, 코드 기반(Code-based) 7종, 다변수 기반(Multivariate-based) 4종, 해시 기반(Code-based) 1종, 아이소제니 기반(Isogeny-based) 1종, 영지식 증명 기반(Zero Knowledge-based) 1종으로 구성되어 있다. 2020년 상기 암호 알고리즘에 대한 평가가 실시될 예정이며, 이후 4종의 표준 암호가 지정될 것으로 예상된다.

표 1. 양자내성암호 표준 공모전 1차 후보군의 종류
Table 1. Type of 1 Round Candidates for NIST Post-Quantum Cryptography Standardization

Algorithm	Encryption /KEM	Sign	Total
Lattice-based	23	5	28
Code-based	17	3	20
Multivariate-based	2	8	10
Isogeny-based	0	1	1
Hash-based	0	3	3
Other	5	2	7
Total	21	48	69

표 2. 양자내성암호 표준 공모전 2차 후보군의 종류
Table 2. Types of 2 Round Candidates for NIST Post-Quantum Cryptography Standardization

Algorithm	Encryption /KEM	Sign	Total
Lattice-based	9	3	12
Code-based	7	0	7
Multivariate-based	0	4	4
Isogeny-based	1	0	1
Hash-based	0	1	1
Zeroknowledge proof	0	1	1
Total	17	9	26

Ⅲ. 하드웨어 구현 동향 및 분석

본 장에서는 기존 양자내성암호 하드웨어 구현 사례 및 표준 공모전 하드웨어 구현 결과물 6종에 대한 동향에 대해 알아보고 각 알고리즘의 성능 평가 결과에 대해 비교 분석하고자 한다. 양자내성암호 표준 공모전의 경우 하드웨어 구현물은 평가 대상이 아니므로 대다수의 알고리즘이 해당 내용을 포함하고 있지 않다.

3.1 양자내성암호 Encryption/KEM 하드웨어 구현 동향

3.1.1 FrodoKEM

Howe, J. et al.[10]에서는 격자 기반 KEM(Key Encryption Mechanism)방식인 FrodoKEM에 대해 Xilinx Artix-7 FPGA 환경상의 하드웨어 구현 결과를 제시하고 있다. 행렬 곱셈의 경우 vector-matrix 곱셈기를 활용하여 구현하였으며, 2개의 cSHAKE 모듈과 1개의 AES 모듈을 사용하고 있으며, 병렬 연산이 가능한 구조로 설계되어 있다. 키 생성, Encapsulation, 그리고 Decapsulation의 모듈이 유사한 동작을 수행하므로 면적 최소화가 가능한 것이 특징이다.

3.1.2 Lizard

J. H. Cheon. et al.[8]에서는 Lizard.CPA와 RLizard.CPA에 대한 최적화 구현 결과를 제시하고 있다. Lizard의 경우 비교적 간단한 계산과 자원에 대한 공유가 용이하다는 장점으로 인해 AES에 비해 더 작은 면적을 가지고 있다. 하지만 매개변수의 크기로 인해 많은 메모리와 레지스터를 사용한다는 단점이 있다.

부산대학교 정보보호 및 지능형 IoT연구실에서는 양자내성암호 표준 공모전 1차 후보군 Lizard.CCA 및 RLizard.CCA에 대한 하드웨어 구현 연구를 진행하였다. 기존의 연구 결과[8]에 대한 하드웨어 설계 및 최적화 구현을 통한 FPGA환경 상에서의 성능 결과를 보이고 있으며, RLizard의 경우 Polynomial Multiplication에 대한 최적화 연산 기법을 적용하였다.

그림 1의 (a)는 Polynomial Multiplication 연산 과정을 나타내는 그림이다. 기존의 연산 수행 시 최대 차수 이상의 계수에 대한 Reduction 연산이 수행되게 되며, Reduction 연산 시 많은 연산 시간을 소모한다.

www.dbpia.co.kr

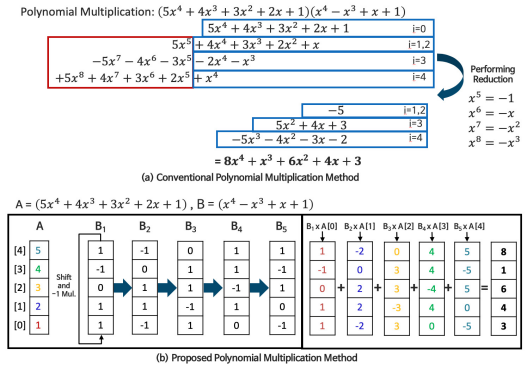

그림 1. 기존의 다항식 곱셈 연상 방법 및 제안하는 기법
Fig. 1. Conventional Polynomial Multiplication Method and Proposed Method

따라서 상기 연구에서는 이러한 다항식 연산 기법에 대한 최적화 기법을 적용하였다. 그림 1의 (b)는 다항식 연산 시 다항식 A와 B의 계수만을 연산에 사용하며, 다항식 B의 경우 [4] 요소는 Shift 연산 및 -1 곱셈 연산을 실시한다. 반복 연산을 통해 생성된 값은 A의 각 계수와 곱셈 연산을 수행하고 모두 더하게 되면 최종적으로 $8x^4+x^3+6x^2+4x+3$가 생성된다. RLizard에서 기존 방법의 경우 16개의 데이터를 처리할 경우 10242의 곱셈 및 Reduction 연산을 수행하며, 제안된 기법의 경우 1024 x 64회의 곱셈 연산을 사용하므로 연산 시간을 줄일 수 있다.

그림 2는 제안기법을 적용한 RLizard.CCA 및 Polynomial Multiplication 연산을 위한 하드웨어 구조를 나타낸다. 10비트 CNT의 상위 6비트 값과 ADDR 간의 비교 연산을 수행한다. ADDR이 작은 경우 Mask 비트를 0으로 처리하고 Mask 비트가 1인 경우 1로 처리하는 구조이며, 메모리에 연산 결과를 누적시키는 구조이다.

3.1.3 Niederreiter Cryptosystem

Wang, W. et al.[12]에서는 Binary Goppa Code를 사용하는 코드 기반 양자내성암호 Niederreiter에 대한 Stratix V FPGA 환경상의 최적화 구현 연구를 기술하고 있다. 1986년 Harald Niederreiter가 개발한 McEliece[13]의 개선된 형태를 보이고 있으며, Binary Goppa Code를 사용하여 안전성을 향상시켰다. uniformly distributed permutation 연산 후 병합 정렬을 통해 고속연산이 가능하며, Gao-Mateer additive FFT(Fast Fourier Transform) 및 Timing 공격에 강인한 Berlekamp-Massey 알고리즘을 구현 결과로 제시하고 있다. 2015년 발표되었던 McEliece[14]와 비교하여 30%의 면적 최소화, 그리고 고속의 복호화 성능을 제시하고 있다.

3.1.4 SIKE(Supersingular Isogeny Key Encapsulation)

양자내성암호 표준 공모전 2차 후보군 알고리즘 SIKE[21]는 Xilinx Virtex-7 FPGA 보드 환경상에서의 최적화 하드웨어 구현 결과를 제시하고 있다. 고속의 아이소제니 계산을 위해 몽고메리 곡선상에서의 효율적인 곱셈 기법과 트리 순회 알고리즘을 사용하였다.

3.2 양자내성암호 서명 하드웨어 구현 동향

3.2.1 SPINCS-256

Amiet et al.[18] 에서는 Kintex-7 Xilinx FPGA 보드 환경 상에 SPHINCS-256 해시 기반 서명 기법의

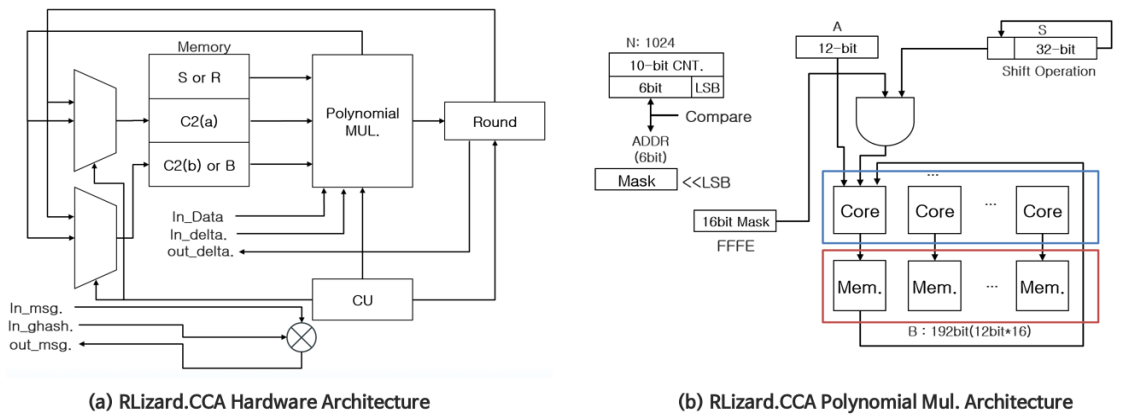

그림 2. RLizard.CCA 하드웨어 구조 및 다항식 곱셈기 구조
Fig. 2. RLizard.CCA hardware structure and polynomial multiplier structure

www.dbpia.co.kr

FPGA 하드웨어 최적화 구현 방식 및 결과를 제시하고 있다. SPHINCS-256에 사용되는 주요 연산은 BLAKE-256, BLAKE-512, 그리고 ChaCha12이다. 해당 논문에서는 최적화 구현을 위해 ChaCha12에 대한 파이프라인 연산 처리 및 관련 Critical Path 최소화 구현을 적용하였다. 제안 기법의 면적 및 동작 수행 성능은 기존 RSA 기반의 서명 방식에 비해 월등한 성능을 보이고 있으며, 실제로 서명 시 1.53ms, 서명 검증에는 65us가 소요된다.

3.3 양자내성암호 키 교환 알고리즘

3.3.1 SIDH(Supersingular Isogeny Diffie-Hellman)

Koziel, B. et al.[17]에서는 SIDH(Supersingular Isogeny Diffie-Hellman)에 대한 최초의 Constant time 하드웨어 구현 논문이다. 고속의 곱셈 연산을 위해 High-Radix Montgomery 곱셈기를 활용하였으며, 병렬처리를 통해 성능을 극대화하였다. 이를 통해 기존 인텔 하스웰(Haswell) 프로세서 상에서 동작하는 SIDH[9]보다 48%의 속도 향상 결과를 제시하고 있다.

Koziel, B. et al.[16]에서는 Constant time SIDH에 대한 FPGA 구현 기법 및 성능평가 결과를 제시하고 있다. Quadratic Extension Field Arithmatic과 아이소제니 계산에 대한 효율적인 병렬처리 연산에 대해 소개하고 있다. 탐욕 알고리즘(Greedy Algorithm)을 구현하여 곱셈, 덧셈, 그리고 중요 연산에 대한 효율적인 병렬 연산이 가능하도록 하였으며, 타이밍 공격에 대응하기 위해 Constant time 연산이 가능하도록 구현되었다. 기존 소프트웨어 구현 결과[9]보다 2배 빠른 연산 속도를 나타내고 있으며, 초기 하드웨어 구현 연구 결과[17] 보다 약 1.3배 빠른 결과를 제시하고 있다.

3.3.2 NewHope-Simple Key Exchange

Oder, T. et al.[6]에서는 격자기반 키 교환 알고리즘인 NewHope-Simple Key Exchange에 대한 구현 결과를 제시하고 있다. NewHope[7]에서 사용하는 NTT(Number Theoretic Transform) 연산에 대한 최적화를 수행하였다. forward transform과 backward transform에 대해 각각 Cooley-Tukey butterfly방식과 Gentleman_Sande butterfly 방식을 적용하였다. 또한 Point-Wise 곱셈 및 Binomial Sampling 과정상에서 최적화 구현을 통해 고속연산이 가능하도록 하였다. 모든 연산은 Constant time에 수행이 되어 타이밍 공격에 대한 안전성을 보장하고 있다. 해당 논문에서 사용되는 파라미터는 표 5과 같다.

3.4 양자내성암호 하드웨어 구현 결과 비교 분석

표 3, 표 4, 표 5는 1, 2, 3절에서 소개한 양자내성암호 하드웨어 구현물에 대한 파라미터를 나타낸다. 일반적으로 격자 기반 암호 알고리즘의 경우 키의 크기가 대체로 큰 것을 확인할 수 있다. 그 중 Lizard.CCA의 키 크기가 가장 크며, 이로 인해 격자기반 양자내성암호의 하드웨어 구현 시 메모리 관리가 요구된다.

표 3. 양자내성암호 암호화/키캡슐화 알고리즘의 파라미터
Table 3. The Parameters of The Post-Quantum Cryptography Encryption/KEM Algorithm

(단위 : byte)

Algorithm	Secret Key	Public Key	Plain text	Cipher text
FrodoKEM-640 FrodoKEM-976	19,872 31,272	9,616 15,632	-	9,736 15,768
Lizard.CCA N1088	557,056	6,553,600	64	3,328
RLizard.CCA Category 5	513	8,192	64	8,512
Niederreiter	5,632	102,987	64	384
SIKEp503 SIKEp751 SIKEp964	434 644 826	378 564 726	-	402 596 766

표 4. SPHINCS-256 서명 알고리즘의 파라미터
Table 4. The Parameters of the SPHINCS-256 Signature Algorithm

(단위 : byte)

Algorithm	Private key	Public Key	Signature size
SPHINCS-256	1,088	1,056	41,000

표 5. 양자내성암호 키 교환 알고리즘의 파라미터
Table 5. The Parameters of the Post-Quantum Cryptography Key Exchange algorithm

(단위 : byte)

Algorithm	Secret key	Public Key	Shared Secret
SIDHp503 SIDHp751	32 48	378 564	126 188
NewHope	1,792	1,824	2,176

www.dbpia.co.kr

표 6에서는 1, 2, 3절에서 기술한 양자내성암호 알고리즘의 성능 평가 결과를 나타내고 있다. 각 알고리즘별로 상이한 성능 평가 환경으로 인해 알고리즘에 대한 객관적 성능 평가가 어려우나 Lizard 암호 알고리즘의 면적 성능이 가장 우수한 것으로 보인다.

Lizard.CPA의 경우 키 생성 시 많은 시간이 소요된다는 단점이 있으나 암·복호화 시간이 짧은 장점이 있다. Ring기반의 Lizard 암호 알고리즘 RLizard.CPA는 타 암호 알고리즘보다 키 생성 및 암·복호화의 연산 시간이 가장 빠르다.

Niederreiter[12]는 기존의 복호화 최적화 구현 결과[14]보다 2배 빠른 Cycle 수치를 보이고 있으며, 면적의 경우 30% 감소, 실제 연산 시간은 3배 이상 빠른 것으로 나타난다.

SIDH[15]의 경우 기존에 연구되었던 소프트웨어 구현 결과[9]보다 2배 빠른 연산 속도를 나타내고 있으며, 초기 하드웨어 구현 연구 결과[17]보다 약 1.3배 빠른 결과를 제시하고 있다.

Ⅳ. 결론 및 향후 연구 방향

본 논문에서는 최신 양자내성암호 하드웨어 구현 결과물 7종에 대한 구현 동향을 알아보고 각 알고리즘의 성능을 비교 분석하였다. 현재 양자내성암호 표준 공모전에서는 소프트웨어 구현에 대한 평가를 진행하고 있으며, 많은 소프트웨어 최적화 구현 연구가

표 6. 양자내성암호 하드웨어 구현물 성능 평가 결과
Table 6. Performance evaluation of Post-Quantum Cryptography Hardware Implementation

Algorithm		Freq. (MHz)	Cycle (x 103)	LUTs	FFs	BRAMs	DSPs	Time (ms)
Encryption/KEM								
FrodoKEM-640[10]	KeyGen	167	3,276	3,771	1,800	6	1	-
	Encaps	167	3,317	6,745	3,528	11	1	-
	Decaps	162	3,358	7,220	3,549	16	1	-
FrodoKEM-976[10]	Keypair	167	7,620	7,139	1,800	8	1	-
	Encaps	167	7,683	7,209	3,537	16	1	-
	Decaps	162	7,745	7,773	3,559	24	1	-
Lizard.CCA (N1088)	KeyGen	100	73,601	3,166	578	70	-	736.01
	Enc.		208					2.08
	Dec.		452					4.52
RLizard.CCA (Category 5)	KeyGen		260	3,072	2,106	6.5	-	2.6
	Enc.		520					5.2
	Dec.		782					7.82
Niederreiter[12]	KeyGen	160	4,929	-	-	-	-	30
	Enc.		10.228					0.06
	Dec.		2.515					0.02
SIKEp751[21] (multiplier = 8)	KeyGen	198	1,798	44,822	51,914	56.5	376	33.35
	Encaps		3,221					
	Decaps		3,383					
Sign								
SPHINCS-256[18]		525	-	19,067	38,132	36	3	1.53
Key Exchange								
SIDH[16] (multiplier = 12)	p503	207	2,940	33,969	45,615	40	384	14.2
	p751	201.5	6,370	50,084	69,054	54.5	576	31.6
NewHope-Simple[6]	Server	125	171.124	5,142	4,452	4	2	1.4
	Client	117	179.292	4,498	4,635	4	2	1.5

www.dbpia.co.kr

진행되고 있다[26,23]. 하지만 그에 비해 하드웨어 구현에 대한 연구는 미진한 편이며 현재 26종의 2차 후보군 중 하드웨어 구현에 대한 결과를 제시하는 알고리즘은 2종에 불과하다. 그러나 양자내성암호 하드웨어 구현 관련 논문들이 점차 출판되고 있으며, 객관적인 하드웨어 구현물에 대한 평가를 위한 표준 API 제정을 위한 연구[24,25] 및 하드웨어 구현 성능 평가 프레임워크[22]에 대한 연구가 이루어지고 있다. 향후에는 기존에 연구되었던 양자내성암호 하드웨어 구현 결과를 바탕으로 향후 2차 후보군에 대한 하드웨어 최적화 구현 및 고속연산을 위한 병렬처리 연구가 활발히 진행될 것으로 보이며, 부채널 분석 및 대응 방안에 대한 연구들도 함께 진행될 것으로 예측된다.

References

[1] L. K. Grover, “A fast quantum mechanical algorithm for database search,” in *Proc. 28th Annu. ACM Symp. Theory of Computing*, pp. 212-219, Philadelphia, USA, May 1996.

[2] P. W. Shor, “Algorithm for quantum computation: Discrete logarithms and factoring,” in *Proc. 35th Annu. Symp. Foundations of Comput. Sci.*, pp. 124-134, Santa Fe, USA, Nov. 1994.

[3] L. Chen, S. Jordan, Y. K. Liu, D. Moody, R. Peralta, R. Perlner, and D. Smith-Tone, *NISTIR 8105 Report on Post-Quantum Cryptography*, Retrieved Feb. 20, 2018, from http://dx.doi.org/10.6028/NIST.IR.8105

[4] G. Alagic, J. Alperin-Sheriff, D. Apon, D. Cooper, Q. Dang, Y. K. Liu, C. Miller, D. Moody, R. Peralta, R. Perlner, A. Robinson, and D. Smith-Tone, *NISTIR 8240 Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process*, Retrieved Feb. 20, 2018, from https://doi.org/10.6028/NIST.IR.8240

[5] M. Ajtai, “Generating hard instances of lattice problems,” in *Proc. The 28th Annu. ACM Symp. Theory of Comput.*, pp. 99-108, Philadelphia, USA, May 1996.

[6] T. Oder and T. Güneysu, “Implementing the NewHope-Simple key exchange on Low-Cost FPGAs,” in *Proc. Cryptology – LATINCRYPT 2017*, La Habana, Cuba, Sep. 2017.

[7] E. Alkim, L. Ducas, T. Pöppelmann, and P. Schwabe, “Post-quantum key exchange-a new hope,” in *Proc. 25th USENIX Secur. Symp. 2016*, pp. 327-343, Texas, USA, Aug. 2016.

[8] J. H. Cheon, S. Park, J. Lee, D. Kim, Y. Song, S. Hong, D. Kim, J. Kim, S.-M. Hong, A. Yun, J. Kim, H. Park, E. Choi, K. Kim, J. S. Kim, and J. Lee, *Post-Quantum Cryptography Round 1 Submissions Lizards*, Retrieved Mar. 1, 2019, https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-1-Submissions

[9] C. Costello, P. Longa, and M. Naehrig, “Efficient algorithms for supersingular isogeny diffie-hellman,” in *Proc. 36th Annu. Int. Cryptology Conf.*, pp. 572-601, California, USA, Aug. 2016.

[10] J. Howe, T. Oder, and T. Güneysu, “Standard lattice-based key encapsulation on embedded devices,” *IACR Trans. Cryptographic Hardware and Embedded Syst.*, vol. 2018, no. 3, pp. 372-393, Feb. 2018.

[11] R. J. McEliece, “A public-key cryptosystem based on algebraic,” *Coding Thv*, pp. 114-116, 1978.

[12] W. Wang, J. Szefer, and R. Niederhagen, “FPGA-based Niederreiter cryptosystem using binary Goppa codes,” in *Proc. The Ninth Int. Conf. Post-Quantum Cryptography*, pp. 77-98, Fort Lauderdale, Florida, Apr. 2018.

[13] H. Niederreiter, “Knapsack type cryptosystems and algebraic coding theory,” *Problems of Contr. and Inf. Theory*, vol. 15, no. 2, pp. 159-166, Jan. 1986.

[14] P. M. C. Massolino, P. S. L. M. Barreto, and V. Wilson, “Optimized and scalable co-processor for McEliece with binary Goppa codes,” *ACM Trans. Embedded Comput. Syst.*, vol. 14, no. 3, May 2015.

[15] H. Yi and Z. Nie, “High-speed hardware architecture for implementations of multivariate signature generations on FPGAs,” *EURASIP J. Wireless Commun. and Netw.*, vol. 2018, no. 1, pp. 1-9, Dec. 2018.

[16] B. Koziel, R. Azarderakhsh, and M. M.

www.dbpia.co.kr

Kermani, "A high-performance and scalable hardware architecture for isogeny-based cryptography," *IEEE Trans. Comput.*, vol. 67, no. 11, pp. 1594-1609, Nov. 2018.

[17] B. Koziel, R. Azarderakhsh, and M. M. Kermani, "Fast hardware architectures for supersingular isogeny diffie-hellman key exchange on FPGA," in *Proc. 17th Int. Conf. Cryptology in India*, pp. 191-206, Kolkata, India, Dec. 2016.

[18] D. Amiet, A. Curiger, and P. Zbinden, "FPGA-based accelerator for post-quantum signature scheme SPHINCS-256," *IACR Trans. Cryptographic Hardware and Embedded Syst.*, vol. 2018, no. 1, pp. 18-39, Feb. 2018.

[19] T. Matsumoto and H. Imai, "Public quadratic polynomial-tuples for efficient signature-verification and essage-encryption," in *Proc. Workshop on the Theory and Application of Cryptography Techniques*, pp. 419-453, Davos, Switzerland, May 1988.

[20] D. Jao and L. D. Feo, "Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies," in *Proc. Int. Workshop on Post-Quantum Cryptography*, pp. 19-34, Heidelbeg, Berlin, Nov. 2011.

[21] D. Jao, R. Azarderakhsh, M. Campagna, C. Costello, L. D. Feo, B. Hess, A. Jalali, B. Koziel, B. LaMacchia, P. Longa, M. Naehrig, J. Renes, V. Soukharev, and D. Urbanik, *SIKE*, Retrieved Mar. 1, 2019, https://sike.org

[22] The ATHENa Team, *ATHENa 0.6.5 Tutorial*, Retrieved Feb. 25, 2018, from https://cryptography.gmu.edu/athena/download/ATHENa_tutorial_0.6.5.pdf

[23] T. H. Park, H. J. Seo, J. S. Kim, H. Y. Park, and H. W. Kim, "Efficient parallel implementation of matrix multiplication for lattice-based cryptography on modern ARM processor," *Secur. Commun. Netw.*, vol. 2018, no. 4, pp. 1-10, Sep. 2018.

[24] K. Gaj, *PQC Hardware API & Fair Benchmarking of PQC*, Retrieved Feb. 25, 2018, from http://www.math.fau.edu/pqcrypto2018/images/06.gaj.pdf.

[25] A. Ferozpuri, F. Farahmad, D. Viet, M. U. Sharif, K. Jens-Peter, and K. Gaj, *Hardware API for Post-Quantum Public Key Cryptosystems*, Retrieved Feb. 25, 2018, from https://cryptography.gmu.edu/athena/PQC/PQC_HW_API.pdf.

[26] H. J. Seo, Z. Liu, P. Longa, and Z. Hu, "SIDH on ARM: Faster modular multiplications for faster post-quantum supersingular isogeny key exchange," *IACR Trans. Cryptographic Hardware and Embedded Syst.*, vol. 2018, no. 3, pp. 1-20, Oct. 2018.

박 찬 희 (Chan-hui Park)

2018년 2월 : 대구대학교 컴퓨터공학과 졸업

2018년 3월~현재 : 부산대학교 전기전자컴퓨터공학과 석사과정

<관심분야> 정보보호, IoT, 암호학, FPGA/ASIC

[ORCID:0000-0002-5233-1667]

김 해 용 (Hae-young Kim)

2015년 8월 : 부산대학교 전자공학과 학사 졸업

2017년 8월 : 부산대학교 전기전자컴퓨터공학과 석사 수료

2017년 9월~현재 : 부산대학교 전기전자컴퓨터공학 박사과정

<관심분야> IoT, 하드웨어 보안, 인공지능, ASIC, 플랫폼 보안

[ORCID:0000-0003-2739-206X]

www.dbpia.co.kr

지 장 현 (Jang-hyun Ji)

2016년 2월 : 부산대학교 정보컴퓨터공학과 졸업
2018년 2월 : 부산대학교 전기전자컴퓨터공학과 석사 수료
2018년 3월~현재 : 부산대학교 전기전자컴퓨터공학과 박사과정
<관심분야> IoT보안, 하드웨어 보안, 보안 SoC
[ORCID:0000-0001-7299-9827]

김 호 원 (Ho-won Kim)

1993년 2월 : 경북대학교 공학사
1995년 2월 : 포항공과대학교 공학석사
1999년 2월 : 포항공과대학교 공학박사
2004년 : Ruhr University Bochum, Post Doctorial
1998년~2008년 : 한국전자통신연구원 팀장
2008년~현재 : 부산대학교 전기컴퓨터공학부 교수
<관심분야> 정보보호, 지능형IoT, FPGA/ASIC, 디지털 트윈
[ORCID:0000-0001-8475-7294]

www.dbpia.co.kr