BIKE 핵심 연산 양자회로 최적구현

양유진*, 장경배*, 오유진*, 임세진*, 서화정**

*한성대학교 (대학원생)

*한성대학교 (교수)

Optimal Implementation of Quantum Circuits of Core Operations in BIKE

Yu-Jin Yang*, Kyung-bae Jang*, Yu-Jin Oh*,

Se-Jin Lim*,Hwa-Jeong Seo**

*Hansung University(Graduate student)

**Hansung University(Professor)

요 약

Google, IBM을 비롯한 많은 기업들에 의해 빠르게 개발되고 있는 양자컴퓨터는 소인수분해, 이산로그 문제를 다항 시간 안에 풀 수 있다고 알려진 Shor 알고리즘의 등장과 맞물려 해당 문제에 기반을 두고 있는 공개키 암호 알고리즘의 안전성에 위협이 되고 있다. 다가올 보안적 취약성에 대응하기 위하여 NIST에선 양자 내성 암호 공모전을 주최하였고 4개의 표준화 알고리즘 선정하였고 3개의 코드기반암호를 대체 알고리즘으로 선정하였다. 양자내성암호 전환에 앞서 더욱 중요해질 양자 컴퓨터 환경에서 양자내성암호를 구현하고 궁극적으로 안전성을 테스트하는 일은 상당한 중요성을 갖는다. 이에 본 논문에서는 Round 4 대체 알고리즘 중 하나인 BIKE의 키 생성, 캡슐화 단계에서 사용되는 $GF(2^n)$상에서의 핵심 산술 연산들을 양자 회로로 최적화 구현하고 사용된 자원을 분석한다.

I. 서론

많은 기업들에 의해 양자컴퓨터의 발전이 이뤄지고 있다. 양자컴퓨터 개발 선도 기업 중 하나인 Google은 2019년 양자우월성을 입증한 것을 시작으로 양자 컴퓨터 연산 중 발생하는 오류를 수정하는 작업에 집중하여 2022년 큐비트의 밀도는 높이고 간섭은 줄여 2%대의 낮은 오류율을 달성하였다[1]. IBM은 2019년 27-qubit 양자 프로세서 Falcon을 지나 가장 최근(2022년 11월) 433-qubit 양자 프로세서 Osprey를 공개하였다. 개발은 IBM에서 발표한 양자컴퓨터 개발 로드맵에 따라 순차적으로 이뤄지고 있으며 2025년까지 4000개 이상의 qubit를 제공하는 프로세서 개발을 목표로 두고 있다[2].

이렇듯 양자컴퓨터가 고도화됨에 따라 현존하는 암호 알고리즘의 보안성이 위협받고 있다. 이 가운데 지수시간이 걸리는 소인수분해, 이산로그 문제를 다항시간에 풀 수 있는 양자알고리즘으로 알려진 Shor 알고리즘의 등장으로 인해 해당 문제들에 기반을 둔 공개키 암호의 안전성을 보장할 수 없게 되었다. 다가올 보안적 취약성에 대응하기 위해서 미국의 국립표준기술연구소(NIST)에선 2017년 양자 내성 암호(PQC) 공모전을 주최하였다. 2022년 7월, 최종적으로 4개의 표준화 알고리즘(격자기반3, 해시기반1)이 선정되었고, 격자기반암호에 집중되어 있는 문제에 대한 대안으로 코드기반암호 3개를 Round 4 대체 알고리즘으로 선정하였다. 현재(2023년 5월 기준) NIST는 PQC 표준화 알고리즘에 대한 문서화 작업과 전자서명 알고리즘에 대한 추가 공모를 진행 중이다[3, 4]. 양자내성암호로의 전환에 앞서 앞으로 더 큰 파이를 차지하게 될 양자 컴퓨터 환경에서 양자내성암호를 구현하고, 궁극적으로

그 안전성에 대해 테스트하는 일은 상당히 중요하다.

이에 본 논문에서는 NIST 양자내성암호 공모전 Round 4의 대체 암호 알고리즘 중 하나인 BIKE의 키 생성, 캡슐화 단계에서 사용되는 $GF(2^n)$상에서의 핵심 산술 연산을 양자 회로로 최적화 구현하고, 각 단계에 사용된 양자 자원을 추정 및 분석한다.

II. 관련연구

2.1 BIKE

BIKE[5]는 NIST의 양자내성암호 공모전에서 대체 후보 알고리즘으로 최종 선정된 암호로, QC-MDPC(Quasi-cyclic Moderate-density parity-check) 코드를 기반으로 하는 KEM(Key Encapsulation Mechanism)이다. QC-MDPC 코드는 준순환 행렬 형태로 나타내기 위해 첫 번째 행에 모든 정보를 담고 있다. 해당 행만 저장하면 행렬의 모든 정보를 저장할 필요가 없기 때문에 공개키의 크기가 작은 편이다. 또한 준순환 행렬의 경우 행렬 곱셈과 인코딩의 속도가 훨씬 빠르다는 특징도 갖는다. 하지만 메시지 복구를 위해 에러를 제거해주는 디코딩 알고리즘이 실패할 수 있는 확률이 존재한다는 점에서 단점을 갖는다.

[표 1]은 BIKE의 파라미터 값을 정리한 것이다. 앞에서부터 블록, 행 가중치 값, 에러 가중치 값, 공유키의 크기를 의미하며, DFR(Decryption Failure Rate)은 오류 정정에 실패할 확률을 의미한다.

Security	r	w	t	l	*DFR*
Level 1	12,323	142	134	256	2^{-128}
Level 3	24,659	206	199		2^{-192}
Level 5	40,973	274	264		2^{-256}

[표 1] BIKE 보안 레벨별 파라미터 크기

2.2 $GF(2^n)$상에서의 산술 연산

$GF(2^n)$는 서로 다른 원소 2^n개를 포함하는 유한체로 n 차수 이하의 다항식으로 표현이 가능하다. 기약다항식(irreducible polynomial)은 더 이상 인수분해가 되지 않는 가장 작은 식으로, 대부분의 암호의 기반으로 사용된다. 이런 이진 필드에서의 산술 연산은 일반적으로 아는 산술 연산과 다소 차이가 있다. 덧셈의 경우 AND와 OR 게이트로 구성된 덧셈기를 사용하는 대신 간단하게 XOR을 사용하며 캐리가 발생하지 않는다는 특징이 있다. 곱셈도 덧셈과 마찬가지로 캐리가 발생하지 않으며 덧셈과는 어떤 곱셈기를 사용하느냐에 따라 성능이 달라지기 때문에 카라추바, 스쿨북, 몽고메리 등 곱셈 알고리즘을 적용한 다양한 곱셈기가 제안되었다. 제곱 연산의 경우 기약다항식의 모듈러 감소를 적용하여 생성된 행렬을 이용한다. 선형 연산이기 때문에 XOR만 사용하여 구현할 수 있으며, PLU 분해를 이용해서 in-place 구조로도 구현이 가능하다. 역치(inversion)연산은 확장 이진 최대공약수 알고리즘(EBGA)이나 Itoh-Tsuji Inversion 알고리즘[6]을 사용하여 구현이 가능하다. 특히 Itoh-Tsuji 알고리즘은 곱셈과 제곱 연산이 같이 사용되기 때문에 이진 유한체 상에서 가장 높은 계산 복잡도를 가진다.

III. BIKE 양자 구현

BIKE는 크게 키 생성, 캡슐화, 역캡슐화 과정으로 구성되어 있다. 본문에서는 이 중 실패 확률이 존재하지 않는 키 생성과 캡슐화 과정만 다뤘으며 가장 핵심이 되는 연산을 양자 회로로 구현하며 사용되는 양자 자원을 계산하였다. 양자 회로 구현에는 IBM에서 제공하는 양자프로그래밍 도구인 ProjectQ를 이용하였다.

BIKE는 가장 낮은 레벨마저도 $GF(2^{12322})$ 환경에서 진행되기 때문에 실제 양자 시뮬레이터로 실행을 할 수 없을 정도로 많은 자원을 요구한다. 이러한 이유에서 구현이 가능하도록 필드의 크기를 축소하였다. 설계원리에 따르면 $GF(2^{r-1})$상에서 기약다항식 $f(X)$는 $(X^r-1)/(X-1)$이고, 블록 길이를 의미하는 r은 소수여야 한다. 구현을 위하여 $r=13$으로 가정하였으며 그에 따른 기약다항식은 아래와 같다.

$$f(X)=X^{12}+X^{11}+\cdots+X^2+X+1$$

3.1 키 생성

키 생성 파트에서 가장 핵심은 공개키 h를 구하는 것이다. 공개키 h는 sparse vector를 통해 생성된 개인키 h_0, h_1로 구성되며, 2가지의 개인키를 이용하여 공개키를 생성하는 식은 $h = h_1 h_0^{-1}$이다. 이 계산을 위해서는 h_0의 역원을 구하는 역치 연산과 h_1과 h_0^{-1} 사이의 곱을 구하는 곱셈 연산이 필요하다.

h_0의 역원은 Itoh-Tsuji Inversion 알고리즘을 적용하여 구할 수 있다. Itoh-Tsuji 알고리즘은 곱셈 연산과 제곱 연산으로 구성되어 있는데, 곱셈 연산에는 Jang et al.이 제안한 이진 유한체상에서의 양자 곱셈기를[7] 활용하였다. 해당 양자 곱셈기는 카라추바 곱셈 알고리즘을 재귀적으로 적용하여, 사용되는 Toffoli 게이트 수를 감소시키고, 추가적으로 보조 큐비트를 할당하여 병렬로 곱셈을 진행함으로써 Toffoli-depth를 1로 최적화한 곱셈기이다. [7]의 곱셈기는 CNOT 게이트와 Toffoli 게이트로 구성되며 본 구현 환경에 맞도록 324개의 보조 큐비트를 추가적으로 할당하였다.

제곱 연산기는 기약다항식으로 생성된 in-place 구조의 행렬을 토대로 CNOT 게이트와 SWAP 게이트를 사용하여 구현하였다. SWAP 게이트의 경우 비용을 차지하지 않기 때문에 제곱 연산의 비용은 CNOT 게이트 수에 의해 결정된다. h_0의 역원을 구하기 위해 Itoh-Tsuji 알고리즘을 적용하면 h_0의 역원은 아래 식으로 표현할 수 있다.

$$h_0^{-1} = h_0^{4094} = ((h_0 h_0^2)^{512}(h_0 h_0^2)^{128}(h_0 h_0^2)^{32}(h_0 h_0^2)^{16}(h_0 h_0^2)^2 h_0)^2$$

위 식에 맞게, 구현한 제곱 연산기와 곱셈기를 적용하여 h_0의 역원 h_0^{-1}를 구하였다. 이 다음 h_0^{-1}과 h_1를 입력으로 양자 곱셈기를 사용하여 공개키 h를 구하였다.

3.2 캡슐화

암호화를 수행하는 캡슐화 과정에서는 암호문 c를 구하는 것이 가장 핵심이다. 랜덤으로 결정되는 에러벡터 e_1과 공개키 h를 곱하고 그 결과값을 또 다른 에러벡터 e_0와 더해주면 첫 번째 암호문 c_0를 얻을 수 있다. 이후 e_0, e_1를 SHA3-384를 사용하는 해시함수 L에 넣어 나온 결과값이 e_0에 저장된다고 가정하고 e_0를 제어큐비트로, 메시지 m을 타겟큐비트로 지정하여 CNOT 게이트 연산을 진행해주면 두 번째 암호문 c_2가 나온다. 암호문 c는 c_1과 c_2가 합쳐진 것이다.

3.3 회로 구현 결과 분석

[표 2]는 $\mathbb{F}_{2^{12}}/(X^{12}+X^{11}+\cdots+X+1)$상에서 BIKE의 각 단계별 핵심 산술 연산들 양자 회로로 구현할 때 사용된 양자 자원을 표로 정리한 것이다. 핵심 산술 연산들에는 역치 연산과 곱셈 연산, 덧셈 연산이 해당한다. 표에서 #T는 T 게이트의 수를 의미하고, #lqcliff는 Clifford 게이트 수로 T게이트를 제외한 나머지 게이트인 CNOT, H, X 게이트의 수를 더한 것이다.

Step	Qubits	#lqcliff	# T	T-depth	Full depth
KeyGen (Inversion & Multiplication)	468	5,719	2,268	20	300
Encaps (Multiplication & Addition)	186	951	378	4	40

[표 2] $\mathbb{F}_{2^{12}}/(X^{12}+X^{11}+\cdots+X+1)$상에서 BIKE의 단계별 핵심 산술 연산의 양자 회로 구현 결과

[표 2]를 보면 대체적으로 키 생성 단계에서 양자 자원이 많이 사용된 것을 볼 수 있다. 이는 해당 단계에서 산술 비용 중 가장 높은 비용을 차지하는 곱셈기 연산이 주를 이루고 있기 때문이다. 캡슐화 단계에서도 자원에 가장 큰 비율을 차지하고 있는 부분이 바로 곱셈기 연산이다.

가장 큰 최적화가 진행된 T-depth에 대해 살펴보자면, 우선 본 구현에 사용한 Toffoli 게이트[8]는 8개의 Clifford 게이트와 7개의 T 게이트로 구성되어 있고, T-depth 4이다. 그렇기 때문에 Toffoli-depth가 1인 [7]의 곱셈기는 1번 사용할 때마다 T-depth 4를 갖는다. Toffoli 게

이트는 곱셈기에만 사용이 되는데 키 생성 파트에서 곱셈기가 inversion 연산에서 4번, 개인키 간의 곱에서 1번 총 5개가 사용되기 때문에 T-depth는 4 X 5 = 20이다. 캡슐화 파트에서는 암호문 c_0를 구할 때 1번만 쓰이기에 T-depth는 4를 갖는다.

IV. 결론

본 논문에서는 NIST 양자내성암호 공모전 Round 4의 후보인 BIKE 코드기반암호에 사용되는 $GF(2^n)$상에서의 핵심 산술 연산에 효율적인 제곱 알고리즘[6]과 최적화된 양자 곱셈기[7]를 활용하여 양자 회로를 최적화 구현하였다. 또한, 구현 결과를 바탕으로 각 연산에 사용된 depth, qubit수, 양자게이트 수 등의 양자 자원을 추정하였다. 해당 양자 회로를 통해 BIKE의 보안 강도 분석 연구에 초석이 될 것으로 기대된다.

향후 연구 계획으로는 유한체 필드 $GF(2^r)$의 범위를 지금보다 더 확장하여 양자 회로를 생성하는 연구를 진행할 것이다. BIKE의 각 레벨의 실제 r값을 적용하면 정말 좋겠지만, 아직 양자 컴퓨터 시뮬레이터가 제공하는 자원으로는 실행이 불가능하기 때문에 각 필드 사이즈에 따른 양자 자원들의 증가 경향을 파악하여 최종적으로 BIKE 레벨 1, 3, 5의 양자 회로 구현에 필요로 하는 양자 자원들을 계산해볼 것이다.

V. Acknowledgement

This work was supported by Institute for Information & communications Technology Planning & Evaluation (IITP) grant funded by the Korea government(MSIT) (<Q|Crypton>, No.2019-0-00033, Study on Quantum Security Evaluation of Cryptography based on Computational Quantum Complexity, 100%).

[참고문헌]

[1] Suppressing quantum errors by scaling a surface code logical qubit. Nature, 2023, 614.7949: 676-681.

[2] The IBM Quantum Development Road map, https://www.ibm.com/quantum/roadmap

[3] NIST Post-Quantum Cryptography Project, https://csrc.nist.gov/Projects/post-quantum-cryptography

[4] 유다은, 김준섭, 김기문. "국내·외 양자내성암호 전환 정책 및 상용화 동향" 정보보호학회지 33, 1 (2023) : 59-63.

[5] Aragon, Nicolas, et al. "BIKE: bit flipping key encapsulation: Round 4 Submission" (2022).

[6] Itoh, Toshiya, and Shigeo Tsujii. "A fast algorithm for computing multiplicative inverses in GF (2m) using normal bases." Information and computation 78.3 (1988): 171-177.

[7] K. Jang, W. Kim, S. Lim, Y. Kang, Y. Yan and H. Seo, “Optimized Implementation of Quantum Binary Field Multiplication with Toffoli Depth One”, International Conference on Information Security Applications, 2022.

[8] Amy, Matthew, et al. "A meet-in-the-middle algorithm for fast synthesis of depth-optimal quantum circuits." IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems 32.6 (2013): 818-830.