정 보 보 호 학 회 지
제 32 권 제2호, 2022. 4

사물인터넷을 위한 경량암호와 양자컴퓨터

장 경 배*, 김 현 지*, 송 경 주*, 양 유 진*, 임 세 진*, 서 화 정**

요 약

사물인터넷 상에서 활용되는 경량암호알고리즘은 높은 보안성과 함께 가용성을 제공할 수 있다는 장점으로 인해 활발히 연구되고 있다. 하지만 경량암호알고리즘은 양자컴퓨터 상에서의 Grover 알고리즘에 의해 해킹될 가능성을 가지고 있다. IBM 그리고 Google을 선두로 한 국제 대기업 및 국가 단위의 연구진들의 활발한 연구로, 고성능 양자 컴퓨터 ‘개발이 앞당겨지고 있다. 공개키 암호와 달리, 대칭키 암호는 양자 컴퓨터로부터 안전하다고 추정되는 문제를 기반으로 하고 있지만 경량화된 암호화 구조에 의해 심각한 보안 취약점을 야기할 수 있다. 본고에서는 사물인터넷을 위한 경량암호를 실제 해킹할 수 있는 양자컴퓨터의 현재 가용 자원에 대해 확인해 보며 이를 통해 양자컴퓨터의 한계점과 앞으로의 사물인터넷 보안의 안전성에 대해 확인해 보도록 한다.

Ⅰ. 서 론

차세대 컴퓨팅 환경으로 알려진 양자컴퓨터는 높은 연산량이 요구되는 시뮬레이션과 인공지능과 같은 분야에서 기존 슈퍼 컴퓨터를 뛰어넘는 높은 성능을 달성할 것으로 알려져 있다. IBM과 Google을 선두로 하여 양자 컴퓨터 개발에 공격적인 투자를 진행 중이며, 이어 Microsoft 그리고 Amazon 등의 국제 대기업들도 양자 컴퓨터 개발에 적극적으로 투자하는 추세이다.

양자컴퓨터는 현재 암호학계의 상황에서 가까운 미래에 다가올 수 있는 가장 큰 위협으로 여겨진다. 이는 양자컴퓨터가 특정 문제를 효율적으로 모델링하고 해결할 수 있는 자체적인 양자 역학적 특성 때문이다. 이러한 문제들은 고전 컴퓨터로 해결하기 어렵기 때문에 현재로서는 안전한 것으로 여겨지지만, 미래에 고성능의 양자컴퓨터가 개발된다면 현재 암호화 시스템의 안전성은 위협받게 된다. 현대 공개키 암호화 시스템의 심각한 안전성 붕괴는 잘 알려져 있지만, 대칭키 암호의 경우 아직은 안전하다고 평가받고 있다. 하지만 암호 시스템의 구조에 따라 대칭키 암호 또한 양자컴퓨터에 대해 심각한 보안 취약점을 가질 수 있다. 대칭키 암호의 안전성을 훼손시킬 수 있는 가장 잘 알려진 방법은 Grover의 검색 알고리즘[1]을 키 전수조사에 적용하는 것이다. 이 잠재적인 양자 공격은 기존 대칭키 암호의 키 검색에 대한 복잡도를 제곱근($\sqrt{\ }$)으로 감소시킬 수 있다.

미국 국립표준기술연구소 NIST (National Institute of Standards and Technology)는 5단계의 양자 후 대칭키 암호에 보안 레벨을 지정하였다[2]. 각 레벨은 AES와 SHA-3의 보안 레벨들로 정의되며 해당 암호 알고리즘을 해킹하기 위한 구체적인 양자 비용이 명시된다. 이에 최근 암호 학계에서는 양자컴퓨터에 대한 대칭키 암호의 안전성을 평가하는 연구들이 활발히 수행되고 있다. 본고에서는 국제적인 양자컴퓨터 개발 현황 및 특징들에 대해 소개하고 사물인터넷 환경에서 활용되는 경량암호들에 대한 양자컴퓨터 상에서의 암호 해킹에 대해 분석한다.

Ⅱ. 양자컴퓨터의 개발 현황

본 장에서는 양자 컴퓨터 개발에 적극적인 투자를 진행 중인 IBM, Google, Amazon, 그리고 Microsoft의

본 연구는 2022년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. NRF-2020R1F1A1048478, 100%).

* 한성대학교 IT융합공학부 (대학원생, starj1023@gmail.com, 대학원생, khj1594012@gmail.com, 대학원생, thdrudwn98@gmail.com, 대학원생, yujin.yang34@gmail.com,, 대학원생, dlatpwls834@gmail.com,)
** 한성대학교 IT융합공학부 (조교수, hwajeong84@gmail.com)

양자 하드웨어 및 양자 소프트웨어의 개발 현황에 대해 살펴본다.

2.1. IBM

IBM은 2020년 9월에 양자 하드웨어 개발 로드맵을 발표하였으며 [표 1]과 같다[3]. 2017년 1월 5 큐비트 양자 하드웨어 (QPU)인 Canary를 시작으로 2019년 27 큐비트의 Falcon, 2020년 65 큐비트의 Hummingbird를 순서대로 공개하였다. 가장 최근 공개한 QPU는 2021년 11월 22일에 공개한 127 큐비트 양자 프로세서인 Eagle이며 이것은 현재 개발된 양자 컴퓨터 중 가장 많은 큐비트를 가지는 양자프로세서이다. Eagle은 육각형 디자인의 3차원 패키징으로 오류율을 줄이고 인접 큐비트에 연결하여 공동 계산이 용이하도록 설계되었다. 공개된 양자 로드맵에 따르면 IBM은 2022년 433 큐비트 프로세서 Qsprey의 개발을 준비하고 있으며 2024년 이후로 1K-1M의 큐비트 달성을 목표로 하고 있다.

IBM은 2000년 중반부터 양자컴퓨터의 동작 시간을 늘리고 오류를 제어하는 연구를 진행 중이며 큐비트 수의 달성뿐만 아니라 개발한 하드웨어에 대한 접근성을 높여 사용을 유용하게 만드는 것을 목표로 하고 있다. 이러한 접근성을 높이기 위해 IBM에서는 향후 3년 안에 모든 개발자들이 사용할 수 있는 클라우드 서비스를 생성 및 성능 개선 계획을 가지고 있다.

2.2. Google

Google은 IBM과 함께 양자 컴퓨터 개발의 선두주자로 여겨지고 있다. 2018년도에는 72 큐비트의 양자 프로세서 Bristlecone을 공개하였으며 2019년도에는 실제 프로그래밍이 가능한 양자 프로세서 Sycamore를 공개하였다. Google은 슈퍼 컴퓨터로는 10,000년이 걸릴 것으로 예상되는 난수 증명 작업을 Sycamore를 사용하여 200초만에 성공함으로써 양자 우위를 세계 최초로 달성하였다[4]. 이와 관련하여 이후에 중국이 Sycamore보다 더 높은 정확도로 샘플링 작업을 완료하여 Google의 양자 우위를 넘어섰다. 게이트 오류를 줄여서 안전성을 향상시키는 것이 더 중요함을 보였으며 이에 Google은 현재 낮은 오류로 시스템을 운영할 수 있는 프로세서 개발에 더 집중하고 있는 추세이다.

2.3. Amazon

비교적 양자 컴퓨팅 사업에 늦게 뛰어든 Amazon의 양자컴퓨터 개발은 아직 초기단계이다. 2020년, 양자게이트에 발생하는 오류로 인해 잘못된 결과가 도출되는 문제를 해결하기 위하여 Schrödinger-cat 큐비트 기반의 내결함성 양자 컴퓨터 (fault-tolerant quantum computer) 아키텍처를 설계한 논문을 처음 공개하였다[5]. 이의 후속 연구를 진행하기 위하여 2021년 10월, 공동연구진인 캘리포니아 공과대학 (Caltech) 내에 AWS 양자 컴퓨팅 센터를 만들었다.

AWS 양자 컴퓨팅 센터의 가장 우선적인 목표는 높은 오류율을 상용화 가능한 수준까지 낮춘 내결함성 양자컴퓨터를 구축하는 것이다. 현재, AWS는 오류율을 낮추기 위하여 양자 방해 요소를 완전히 차단하는 소재를 만들어 쌓는 방식과 오류를 보정할 수 있는 아키텍쳐를 통해 프로세서에서 발생하는 오류를 감지하고 수정하는 방식을 연구하고 있다. 이 연구에 대한 구체적인 일정이나 목표 시기 등은 아직 공개되지 않았다.

2.4. Microsoft

큐비트의 형식에 따라 양자 컴퓨터의 구현 방법이 달라지는데 초전도 큐비트를 다루는 IBM 그리고 Google과는 달리 Microsoft는 유일하게 전자의 위상학적 특징을 이용하는 위상 큐비트 기반의 양자 컴퓨터를 개발하고 있다. 위상수학을 이용한 양자컴퓨터는 이론상으로 가장 완벽하다고 평가받고 있으며, 다른 큐비트를 기반으로 하는 양자컴퓨터에 비해 빠른 속도, 작은 크기, 그리고 안전성을 가진다[6]. 올해 3월 Microsoft는 위상

〔표 1〕 IBM 양자 하드웨어 개발 로드맵

년도	2019	2020	2021	2022	2023	2024
양자 프로세서	Falcon	Humming bird	Eagle	Qsprey	Condor	Beyond
큐비트 수	27	65	127	433	1,121	천-만

큐비트의 구현가능성을 보여주는 물리학적 실험을 시연했다 [7]. 양자컴퓨터 구현을 위한 연구를 수행하고 있으며, 많은 시간이 소요될 것으로 보인다.

Ⅲ. 양자컴퓨터 개발 환경 및 SDK

본 장에서는 대표적인 양자 프로그래밍 플랫폼에 대해 살펴보고 각자의 개발 환경 및 특징에 대해 살펴본다.

3.1. IBM Qiskit

IBM Qiskit은 Python 등의 host language와 함께 quantum language인 OpenQASM 과 IBM의 실제 양자 프로세서를 사용하기 위한 오픈 소스 소프트웨어 개발 키트 (SDK)이다 [8]. Qiskit은 IBM Quantum lab과 Circuit composer를 제공한다. 클라우드 서비스인 IBM Quantum Lab은 Python 기반의 Jupyter notebook을 통한 프로그래밍 환경을 제공한다. IBM Quantum Lab을 통해 양자 프로그래밍에 필요한 라이브러리 및 5개의 시뮬레이터 그리고 22개의 양자 프로세서 등을 쉽게 사용할 수 있다. API token을 발급받을 경우 로컬 환경에서도 실제 양자 하드웨어를 사용할 수 있다. 또한, 머신러닝, 화학 등의 분야에 대한 다양한 튜토리얼을 제공한다.

Circuit composer는 큐비트와 양자 게이트가 시각적으로 제공되며, 드래그 앤 드롭 방식을 통해 회로를 직관적으로 구성할 수 있다. 해당 기능은 QASM 및 Qiskit 코드로 자동으로 작성되며, 작성된 코드는 양자 시뮬레이터 및 하드웨어에서 실행이 가능하다. 또한, Circuit composer에서는 큐비트의 상태 벡터, 확률 등을 별도의 작업 없이 즉각적으로 확인할 수 있다.

Qiskit은 다양한 양자 시뮬레이터를 제공하므로 사용 목적과 상황에 맞는 적절한 시뮬레이터를 사용할 수 있다. 그 중 ‘qasm_simulator’는 범용적인 시뮬레이터로, 입력회로 및 매개변수에 따라 시뮬레이션 방법이 선택되며, 양자회로를 실행한 후, 0 또는 1의 상태로 관측된 결과를 얻을 수 있다. ‘statevector_simluator’는 0 또는 1로 결정된 값이 아닌 복소수 형태의 큐비트 상태를 확인할 수 있다. 해당 시뮬레이터는 qubit statevector의 wavefunction을 계산함으로써 양자 회로를 시뮬레이션하는 방식이다. [표 2]는 두 시뮬레이터에 대한 실행시간을 보여준다. Qiskit에서는 최대 32개의 큐비트를 제공한다고 하였으나, 실제 양자 회로를 실행한 결과, 최대 24 큐비트까지 동작 가능하였다.

〔표 2〕 큐스킷 양자 시뮬레이터 실행 속도(회로 depth=30, Shots=30, 단위=초)

큐비트 수	실행 시간	
	Qasm 시뮬레이터	Statevector 시뮬레이터
10	0.02	0.01
20	0.49	0.88
24	10.01	19.9
25	동작 불가	동작 불가

Qiskit은 22 종류의 양자 프로세서를 제공하며, 최대 127 큐비트까지 제공한다. 그러나 5 큐비트의 이상의 양자 프로세서를 사용하기 위해서는 연구자 허가 심사를 받아야 하며 별도의 절차가 필요하다. [표 3]은 5 큐비트를 지원하는 양자 프로세서인 ‘ibmq_manila’를 통해 양자회로를 실행할 경우의 실행 시간이다. 제공하는 5큐비트를 모두 사용할 수 있었으며, 양자 프로세서 사용 시 큐에서 약 1분~15분 정도 대기한 후 실행된다. 이외에도 Qiskit은 시각화 기능, 게이트 최적화, 회로 디버깅, 그리고 노이즈 모듈을 통한 노이즈 모델 시뮬레이션 등과 같이 다른 플랫폼에 비해 양자회로를 중점으로 하여 양자 프로그래밍에 필요한 다양한 기능들을 제공한다.

〔표 3〕 큐스킷 양자 프로세서 마닐라 실행 속도(회로 depth=30, Shots=1024, 단위=초)

큐비트 수	실행 시간
3	956.68
5	845

3.2. ProjectQ

ProjectQ는 파이썬 기반의 오픈소스 양자 프로그래밍 플랫폼이다. 기존의 파이썬 명령어와 ProjectQ 라이브러리를 활용하여 다양한 양자 프로그램 및 알고리즘을 구현하고 시뮬레이션할 수 있다. ProjectQ의 장점은 C++ 기반의 시뮬레이터를 사용한 빠른 속도이다. 약 30 큐비트 정도를 사용할 수 있다. ProjectQ 또한 실제 양자 하드웨어에 대한 클라우드 서비스를 이용할 수 있

으며 IBM, IonQ, AES Braket 등이 있다. ProjectQ는 양자 회로를 직접 구현하고 시뮬레이션 및 분석에 용이하지만 양자 인공지능과 같은 심화 라이브러리를 자체적으로 제공하지 않는다.

3.3. Amazon Braket

Amazon은 2019년 12월 2일 관리형 양자 컴퓨팅 서비스 인 Braket을 공개했다 [9]. Braket은 D-wave, IonQ, Rigetti, 그리고 Oxford Quantum Circuit(OQC)와 협력하여 양자 시뮬레이션 및 양자 컴퓨터의 동작을 지원한다. Amazon Braket은 개발 속도를 높이기 위한 양자 컴퓨팅 서비스로서 작동 방식은 Build, Test, Run, 그리고 Analyze로 나눠진다. Build는 Jupyter notebook이나 개인 로컬 작업환경에서 양자 알고리즘을 build하는 과정이며 Test는 로컬 시뮬레이터나 고성능 시뮬레이터에서 알고리즘을 확인한다. Run은 테스트 완료된 양자 알고리즘을 선택한 양자 컴퓨터에서 실행하고 하이브이드 알고리즘을 위해 classical 리소스와 quantum 리소스를 결합한다. 마지막으로 Analyze는 알고리즘이 끝난 후 결과 분석을 수행한다. Amazon Braket은 제공하는 소프트웨어 개발 키트 (SDK)을 사용하여 양자 알고리즘 및 시뮬레이터를 동작할 수 있으며 기본적으로 SDK가 설치된 Jupyter notebook을 제공하여 개발환경 세팅 없이 사용 가능하여 편리하다.

현재 Amazon Braket에서는 일반적인 환경에 대해 최대 50-qubit의 양자 시뮬레이터와 80-qubit의 양자 컴퓨터 사용을 지원한다. 제공하는 local 시뮬레이터는 무료로 최대 25 큐비트를 지원하며, 25 큐비트 모두 동작 가능하다. 그러나, 커널을 재시작하지 않고 회로를 반복적으로 동작시킬 경우 메모리 에러가 발생하여 회로 동작이 불가능하다. [표 4]에서는 local 시뮬레이터의 큐비트 수 별 실행시간을 보여주고 있다.

depth=30의 양자 회로 시뮬레이션 결과 25 큐비트까지 동작 가능했으며 12.48초의 실행 시간을 보였다. 유료로 제공하는 양자 시뮬레이터로 SV1, TN1, 그리고 DM1가 있으며 task의 작업 duration을 기준으로 서비스 사용 비용이 결정된다. SV1 양자 시뮬레이터로 depth=30의 양자회로를 동작시켜 본 결과 34 큐비트까지 동작하였으며 31큐비트 까지는 1분 내외의 짧은 실행시간을 보였지만 32-34 큐비트에 대해서는 약 5분 내외의 실행시간을 보였다.

〔표 4〕 아마존 브라켓 양자 시뮬레이터 실행 속도(회로 depth=30, Shots=1024, 단위=초)

큐비트 수	실행 시간
10	0.02
15	0.03
20	0.32
25	12.48

Braket이 지원하는 양자 컴퓨터로는 Lucy, IonQ, Aspen11 등이 있으며 shot과 task에 대한 기준으로 서비스 비용이 결정된다. 여기에서 shot은 QPU 내에서 양자 알고리즘의 단일 실행을 의미하며 Task는 동일한 회로 혹은 어닐링 문제를 기반으로 하는 반복된 shot, 즉 task를 제출할 때 task에 포함된 모든 shot을 의미한다.

3.4. Microsoft Q#

Q#은 Microsoft에서 제공하는 양자 프로그램 개발 및 실행을 위한 양자 중심 오픈소스 프로그래밍 언어이고, Microsoft QDK (양자 개발 키트)는 클라우드 및 로컬 환경에서 개발이 가능한 Azure Quantum용 오픈 소스 개발 키트이다. QDK에는 Q#이 포함되어 있으며, QDK를 통해 양자 컴퓨팅을 위한 클라우드 서비스인 Azure quantum을 사용할 수 있다. Q#은 Visual Studio, Visual Studio Code 그리고 Jupyter Notebook과의 통합 기능을 제공하며, Python과 기타 .NET 언어와의 상호 운용성을 지원하고 [10], 다양한 라이브러리를 'open' 명령문을 통해 사용할 수 있다. 또한, Qiskit, Cirq와 호환되어 해당 언어로 작성된 프로그램일지라도 Azure quantum을 통해 양자 하드웨어 및 시뮬레이터 상에서 실행시킬 수 있다.

Azure Quantum은 Q# 양자 프로그램을 실행하기 위한 다양한 하드웨어 및 양자 시뮬레이터를 지원한다. 작업영역을 생성한 후 provider를 선택하면 해당 provider를 notebook 형태로 사용할 수 있다. Azure quantum에서 제공하는 provider는 복잡한 얽힘 시스템을 구축할 수 있는 IonQ와 중간 회로 측정 및 큐비트 재사용을 수행하는 기능이 포함된 Honeywell이 있다. IonQ는 29 큐비트를 제공하는 GPU 가속 시뮬레이터와 11 큐비트의 양자 프로세서를 제공하고, Honeywell은 6 큐비트

(System Model H0) 및 10 큐비트 (System Model H1)의 이온 트랩 양자 프로세서를 제공한다 [11, 12].

[표 5]와 [표 6]은 각각 로컬 환경에서의 QDK의 양자 시뮬레이터의 회로 실행 시간과 Azure quantum에서 제공하는 Ion Simulator의 회로 실행 시간이다. QDK 시뮬레이터의 경우 최대 32 큐비트를 지원한다고 하였으나 depth가 30인 양자 회로 실행 시 최대 29 큐비트까지 동작 가능하였으며, qiskit에 비해 더 많은 큐비트를 시뮬레이션 할 수 있었다. 다음으로 Azure quantum의 IonQ 시뮬레이터는 최대 40 큐비트를 제공한다고 하였으나, 다른 시뮬레이터들에 비해 전반적으로 느린 속도를 보였으며, 가끔 비정상적으로 빠르게 수행될 경우도 존재하였다. 또한, 동일 회로를 여러 번 반복 실행 시, 동작이 불가능한 경우도 발생하는 등 불안정한 성능을 보였다.

〔표 5〕 QDK 양자 시뮬레이터 실행 속도(회로 depth=30, 단위=초)

큐비트 수	실행 시간
10	0.5
20	1.5
24	2
28	36
29	79
30	동작 불가

〔표 6〕 Azure IonQ 양자 시뮬레이터 실행 속도(회로 depth=30, 단위=초)

큐비트 수	실행 시간
10	57.34
15	54.57
20	277.85
21	782.84
25	12535.67

Ⅳ. 양자컴퓨터를 활용한 경량암호 상에서의 해킹

본 장에서는 Grover 알고리즘을 사용한 양자 컴퓨터 상에서의 경량암호 해킹에 대해 소개한다. Grover 알고리즘을 사용한 경량암호 해킹은 공격 대상 암호 알고리즘에 대한 양자 회로를 얼마나 효율적으로 구현하는지에 따라 최종 비용이 결정된다. 이에 다양한 경량암호들을 양자 회로로 효율적으로 구현하는 연구들이 수행되고 있다. 4.1장에서는 ARX (Addition, Rotation, XOR) 구조, 4.2장에서는 SPN (Substitution-Permutation Network) 구조의 경량암호 양자 회로 구현에 대해 살펴보고 분석한다. 4.3장에서는 NIST에서 추정한 대칭키 암호에 대한 공격 비용에 대해 분석하고, 지정된 5단계의 양자 후 보안 레벨을 경량암호들에 적용하여 비교해 본다.

4.1. ARX 구조 경량암호 LEA, HIGHT, CHAM에 대한 양자 해킹

ARX 구조를 가진 LEA, HIGHT, CHAM의 양자 회로의 경우, 양자 덧셈을 어떻게 구현하는지에 따라 성능에 큰 영향을 끼친다.

Rotation 연산의 경우, 큐비트간의 인덱스를 변경하는 논리적 Swap을 통해 양자 자원을 전혀 사용하지 않고 회로를 설계할 수 있다. XOR 연산은 일반적으로 CNOT 게이트를 통해 구현된다. 반면에 덧셈 연산은 양자 컴퓨터상에서 사용되기 위해서는 비교적 많은 양자 자원들이 필요하기에 기존 컴퓨터에서와는 달리 복잡한 연산에 속하며 설계 방법이 다양하기 때문에 이를 효율적으로 구현하는 연구들이 다수 발표되고 있다[13, 14].

LEA, HIGHT, 그리고 CHAM에 대한 양자 회로를 구현하고 사용된 양자 자원들에 대해 분석한 연구는 2020년도에 처음으로 수행되었다 [15]. 해당 연구에서는 양자 덧셈을 구현하는데 있어 [14]의 일반적인 ripple carry 양자 덧셈기가 사용되었다. 이후 [16]에서는, [14]의 향상된 ripple-carry 양자 덧셈기를 사용하여 1차적인 성능 개선이 이루어졌으며 암호화 양자 회로를

〔표 7〕 LEA, HIHGT, CHAM에 대한 양자 공격 비용

알고리즘		총 게이트	총 depth	큐비트 수
LEA	128/128	2^{82}	2^{77}	389
	128/192	2^{115}	2^{109}	1,037
	128/256	2^{148}	2^{141}	1,165
HIGHT	64/128	2^{82}	2^{75}	457
CHAM	64/128	2^{81}	2^{76}	409
	128/128	2^{81}	2^{77}	293
	128/256	2^{146}	2^{141}	841

설계하는데 있어 덧셈 연산들을 병렬로 설계하여 높은 성능 향상을 제공하였다. 가장 많은 회로 depth를 차지하는 덧셈들을 병렬로 구현함으로써 LEA, HIGHT, CHAM의 회로 depth를 78%, 85%, 70%씩 감소시켰다. [표 7]은 [16]에서 추정한 LEA, HIGHT, CHAM에 대한 사용한 양자 해킹 비용이다.

4.2. SPN 구조 경량암호 PIPO, GIFT, PRESENT에 대한 양자 해킹

SPN 구조 경량암호의 양자 회로의 경우 대부분은 Sbox 구현에 가장 많은 양자 자원들이 사용된다. Sbox가 효율적으로 구현된다면, SPN 구조의 블록 암호의 양자 회로는 일반적으로 ARX 구조보다 적은 비용으로 구현된다.

고전 컴퓨터에서의 Sbox 구현 시, 입력에 따른 출력을 사전에 정의해두는 사전 테이블 방식은 일반적인 선택 사항이지만, 양자 컴퓨터에서는 그렇지 않다. 모든 입력이 확률로서 존재하는 중첩 상태에서 입력에 대한 출력을 사전에 정의하는 방식의 양자 회로 구현에 많은 비용이 필요하기 때문이다. 따라서 중첩 상태의 모든 입력 값에 대해 모든 출력 값을 계산할 수 있는 Sbox의 수식을 양자 게이트들을 조합하여 구현해야 한다. [표 8]은 SPN 구조의 경량암호 PIPO [17], PRESENT [18], 그리고 GIFT [18]에 대해 추정한 양자 해킹 비용이다.

PRESENT와 GIFT의 양자 회로 구현에서는, 중요 요소인 4-bit Sbox 양자 회로를 구현하는데 있어 LIGHTER-R [19]가 사용되었다. LIGHTER-R은 그래프 기반의 탐색 알고리즘을 사용하여 4-bit 입력에 대한 출력을 계산하는 수식 형태의 Sbox 양자 회로를 생성하는 프로그램이다. 이를 통해 [18]에서는 in-place 방식의 효율적인 Sbox 양자 회로를 구현하였다.

PIPO는 PRESENT와 GIFT와는 다르게 8-bit Sbox가 사용된다. [17]에서는 효율적인 Sbox 양자 회로를 위해 기존 PIPO의 Sbox 수식을 자체적으로 변경하고 리버스 연산을 활용하여 in-place 방식의 효율적인 Sbox 양자 회로를 구현하였다.

[표 7]과 [표 8]을 비교해 보았을 때, SPN 구조 경량암호는 ARX 구조 경량암호보다 적은 비용으로 양자 해킹이 가능하다. 이는 ARX 구조 경량암호의 양자 회로 구현 시, 덧셈에 많은 비용이 소모되며 SPN 구조 경량암호의 양자 회로에서 Sbox가 효율적으로 구현된 편에 속하기 때문이다.

〔표 8〕 PIPO, PRESENT, GIFT에 대한 양자 공격 비용

알고리즘		총 게이트	총 depth	큐비트 수
PIPO	64/128	2^{80}	2^{74}	257
	64/256	2^{145}	2^{139}	513
PRESENT	64/80	2^{56}	2^{51}	209
	64/128	2^{80}	2^{77}	257
GIFT	64/128	2^{80}	2^{74}	257
	128/128	2^{81}	2^{75}	257

4.3. NIST 양자 후 보안 레벨 분석 및 경량암호 보안 레벨 평가

NIST는 AES와 SHA-3의 변형 버전들에 대한 양자 해킹 비용을 기준으로 하여 5단계의 양자 후 보안 레벨을 [표 9]와 같이 지정하였다. Level 1, 3, 그리고 5에 해당하는 AES의 양자 해킹 비용은 2016년도 Grassl et al.이 추정한 AES의 양자 해킹 비용(2^{170}, 2^{233}, 2^{298})[20]을 인용하고 있다. NIST는 Level 2, 4의 SHA에 대해서는 구체적인 비용을 인용하고 있지 않지만 SHA-3-256의 양자 해킹 비용이 AES-192보다 적을 것으로 추측하고 있다. [표 7], [표 8]의 비용과 AES에 대

〔표 9〕 NIST 양자 후 보안 레벨

보안 레벨	요구사항
레벨 1 (2^{170})	**AES-128**를 대상으로한 양자 Grover 알고리즘 공격 비용과 비슷하거나 더 높아야 한다.
레벨 2	**SHA-3-256**를 대상으로한 양자 Grover 알고리즘 공격 비용과 비슷하거나 더 높아야 한다.
레벨 3 (2^{233})	**AES-192**를 대상으로한 양자 Grover 알고리즘 공격 비용과 비슷하거나 더 높아야 한다.
레벨 4	**SHA-3-384**를 대상으로한 양자 Grover 알고리즘 공격 비용과 비슷하거나 더 높아야 한다.
레벨 5 (2^{298})	**AES-256**를 대상으로한 양자 Grover 알고리즘 공격 비용과 비슷하거나 더 높아야 한다.

한 [표 9]의 비용(2^{170}, 2^{233}, 2^{298})을 비교해 보았을 때, 경량암호는 AES보다 상당히 적은 비용으로 양자 해킹에 노출되어 안전성이 제곱근으로 감소된다.

하지만 명시해야할 것은 [표 9]의 AES에 대한 양자 해킹 비용은 2016년도 AES의 최초 양자 회로 구현 결과라는 점이다. 이후 AES의 양자 회로 성능을 개선시키는 다양한 연구들이 발표되었다 [21, 22]. 이 중, EUROCRYPT'20에서는 AES-128에 대한 비용을 가장 많이 감소시켰다 [21]. 구현과 사용 양자 자원 추정에 대한 몇 가지 오류가 존재하긴 하지만 2^{157}까지 양자 해킹 비용을 감소시켰다. 이러한 결과로 보아, NIST의 양자 후 보안 레벨에 따른 공격 비용은 보수적으로 추정되었다고 분석할 수 있다. NIST에서는 양자 해킹에 필요한 큐비트 수는 비용 추정에서 고려하고 있지 않다. Grover 알고리즘은 수많은 양자 회로의 순차적인 반복이 필요하다. 이로 인해 회로 depth와 게이트의 오버헤드는 매우 큰 반면 큐비트는 상대적으로 적다. 다시 말해서 Grover 알고리즘의 특성과 NIST의 추정 방식을 고려해보았을 때 큐비트의 수를 줄이는 구현보다는 회로 depth와 게이트 수를 줄이는 것이 더욱 중요하다는 것을 알 수 있다.

[표 10]은 ARX 구조 경량암호 LEA, HIGHT, 그리고 CHAM 그리고 SPN 구조 경량암호 PIPO, PRESENT, 그리고 GIFT에 대한 양자 후 보안 레벨을 NIST의 지정 기준을 적용하여 평가한 것이다.

〔표 10〕 경량암호에 대한 양자 후 보안 레벨 평가

알고리즘		비용	NIST 보안 레벨
LEA	128/128	2^{159}	Not achieved
	128/192	2^{225}	Level 1
	128/256	2^{289}	Level 3
HIGHT	64/128	2^{158}	Not achieved
CHAM	64/128	2^{157}	Not achieved
	128/128	2^{158}	Not achieved
	128/256	2^{287}	Level 3
PIPO	64/128	2^{154}	Not achieved
	64/256	2^{284}	Level 3
PRESENT	64/80	2^{108}	Not achieved
	64/128	2^{157}	Not achieved
GIFT	64/128	2^{154}	Not achieved
	128/128	2^{156}	Not achieved

동일 키 크기 기준으로 경량암호와 NIST에서 지정한 AES의 양자 해킹 비용을 비교해 본다면, 경량암호는 AES보다 쉽게 양자 해킹에 노출된다. 이는 경량암호가 양자 후 시대에 다가올 안전성 위협에 내성이 적음을 의미한다. 하지만 최신 AES의 양자 해킹 추정 비용을 기준으로 한다면, ARX 구조 경량암호에 대한 양자 해킹에 AES와 비슷하거나 조금 더 높은 비용이 필요하다. SPN 구조의 경우, Sbox가 효율적으로 구현된다면 여전히 AES보다 적은 비용으로 양자 해킹에 노출된다. 이로 미루어 보았을 때, 다가오는 양자 컴퓨터 시대에는 SPN 구조보다는 ARX 구조로 설계된 경량암호가 안전성 위협에 내성을 더 가질 것으로 판단된다.

V. 결 론

가까운 미래에 등장할 고성능 양자 컴퓨터로부터의 안전성 위협을 확인하는 가장 확실한 방법은 양자 공격에 대해 각 암호 알고리즘의 안전성을 평가하는 것이다. 본고에서는 국제적인 양자 컴퓨터 개발 사업에 대한 현황과 이에 다가올 양자 후 시대에서의 사물 인터넷 환경을 위한 경량암호 안전성을 분석하였다. 대칭키 암호화는 양자 컴퓨터로부터 안전하다고 추정되는 문제를 기반으로 하지만 구조에 따라 양자 컴퓨터의 공격으로부터 심각한 보안 취약점을 가질 수 있다. 사물 인터넷 환경에서 경량암호의 양자 후 안전성을 고려하여 암호 시스템을 구축하는 것은 중요한 향후 계획이 될 것으로 사료된다.

참 고 문 헌

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

[2] NIST, "Submission requirements and evaluation criteria for the post-quantum cryptography standardization process," [internet], https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/call-for-proposals-final-dec-2016.pdf.

[3] IBM, “IBM’s roadmap for building an open quantum software ecosystem”[internet], https://research.ibm.com/blog/quantum-development-roadmap

[4] F.Arute, K.Arya, R.Babbush, D.Bacon, J.C.Bardin, R.Barends, and J.M.Martinis, “Quantum supremacy using a programmable superconducting processor,” Nature, 574(7779), pp.505-510, Oct 2019.

[5] Aws, “Designing a fault-tolerant quantum computer based on Schrödinger-cat qubits,” [internet], https://aws.amazon.com/ko/blogs/quantum-computing/designing-a-fault-tolerant-quantum-computer-with-cat-qubits/

[6] Microsoft, “overview understanding quantum computing” [internet], https://docs.microsoft.com/ko-kr/azure/quantum/overview-understanding-quantum-computing

[7] Microsoft, “Microsoft has demonstrated the underlying physics required to create a new kind of qubit,” [internet], https://www.microsoft.com/en-us/research/blog/microsoft-has-demonstrated-the-underlying-physics-required-to-create-a-new-kind-of-qubit/

[8] G. Aleksandrowicz et al, “Qiskit: An Open-source Framework for Quantum Computing (0.7.2),” Zenodo. https://doi.org/10.5281/zenodo.2562111.

[9] C. Gonzalez, "Cloud based QC with Amazon Braket." Digitale Welt 5.2 (2021): 14-17.

[10] “Set up a local development environment for Azure Quantum,” [internet], https://docs.microsoft.com/ko-kr/azure/quantum/install-overview-qdk

[11] “IonQ provider,” [internet], https://docs.microsoft.com/en-us/azure/quantum/provider-ionq#quantum-simulator

[12] “Honeywell provider,” [internet], https://docs.microsoft.com/en-us/azure/quantum/provider-honeywell

[13] T. G. Draper, S. A. Kutin, E. M. Rains, and K. M. Svore, “A logarithmic-depth quantum carry-lookahead adder, ” Quantum Inf. Comput. vol.6, no.4-5, pp. 351-369, 2006.

[14] S, A. Cuccaro, T. G. Draper, S. A. Kutin, D. P. Moulton, “A new quantum ripple-carry addition circuit,” arXiv, https://arxiv.org/%20pdf/quant-ph/0410184.pdf. 2008.

[15] K.B. Jang, S.J. Choi, H.D. Kwon, H.J. Kim, J.H. Park, and H.J. Seo, “Grover on Korean Block Ciphers,” Applied Sciences, vol. 10, no. 18, pp. 6407, Sep. 2020.

[16] K.B. Jang, G.J. Song, H.J. Kim, H.D. Kwon, H,J. Kim, and H.J. Seo, “Parallel Quantum Addition for Korean Block Cipher,” Cryptology ePrint Archive, Report 2021/1507, Nov. 2021.

[17] K.B. Jang, G.J. Song, H.D. Kwon, S.W. Uhm, H,J. Kim, W.K. Lee, and H.J. Seo, “Grover on PIPO,” Electronics, vol.11, no.11, pp. 1194, 2021.

[18] K.B. Jang, G.J. Song, H.J. Kim, H.D. Kwon, H,J. Kim, and H.J. Seo, “Efficient Implementation of PRESENT and GIFT on Quantum Computers,” Applied Sciences, vol.11, no.11, pp. 4776, 2021.

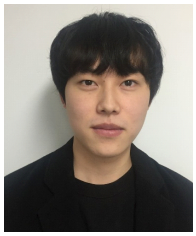
[19] V. A. Dasu, A. Baksi, S. Sarkar, and A. Chattopadhyay, “LIGHTER-R: Optimized Reversible Circuit Implementation For SBoxes,” 2019 32nd IEEE International System-on-Chip Conference (SOCC), pp 260-265, 2019.

[20] M. Grassl, B. Langenberg, M. Roetteler and R. Steinwandt, “Applying Grover’s algorithm to AES: quantum resource estimates,” Post-Quantum Cryptography, PQCrypto'16, LNCS, 9606, pp. 29–43, 2016.

[21] S. Jaques. M. Naehrig, M. Roetteler, and F. Virdia, “Parallel Quantum Addition for Korean Block Cipher,” Cryptology ePrint Archive, Report 2019/1146, Oct. 2019.

[22] B. Langenberg, H. Pham, and R. Steinwandt, “Reducing the Cost of Implementing AES as a Quantum Circuit,” Cryptology ePrint Archive, Report 2019/854, Jul. 2019.

〈저 자 소 개〉



장 경 배 (Kyungnae Jang)
학생회원
2019년 3월 : 한성대학교 IT응용시스템공학부 졸업
2021년 3월 : 한성대학교 IT융합공학부 석사
2021년 3월~현재 : 한성대학교 정보컴퓨터공학과 박사과정
<관심분야> 정보보호, 암호, 양자컴퓨터

김 현 지 (Hyunji Kim)
학생회원
2020년 2월 : 한성대학교 IT융합공학부 졸업
2022년 2월 : 한성대학교 IT융합공학부 석사
2022년~현재 : 한성대학교 정보컴퓨터공학과 박사과정
<관심분야> 정보보호, 인공지능

송 경 주 (Gyeongju Song)
학생회원
2021년 2월 : 한성대학교 IT융합 학부 졸업
2021년 3월~현재 : 한성대학교 IT융합공학부 석사과정
<관심분야> 암호, 양자컴퓨터

양 유 진 (Yujin Yang)
학생회원
2022년 2월 : 한성대학교 IT융합공학부 졸업
2022년 3월~현재 : 한성대학교 IT융합공학과 석사과정
<관심분야> 양자컴퓨터, 정보보안

임 세 진 (Sejin Lim)
학생회원
2022년 2월 : 한성대학교 컴퓨터공학부 졸업
2022년 3월~현재 : 한성대학교 IT융합공학부 석사과정
<관심분야> 인공지능 보안, 정보보안

서 화 정 (Hwajeong Seo)
종신회원
2010년 2월 : 부산대학교 컴퓨터공학과 졸업
2012년 2월 : 부산대학교 컴퓨터공학과 석사
2015년 4월~5월 : 싱가포르 난양공대 인턴쉽
2016년 2월 : 부산대학교 컴퓨터공학과 박사
2017년 3월 : 싱가포르 과학기술청 연구원
2017년 4월~현재 : 한성대학교 조교수
<관심분야> 암호구현