

# 양자컴퓨터 플랫폼 동향

임 세 진\*, 김 현 지\*, 김 덕 영\*, 장 경 배\*, 양 유 진\*, 오 유 진\*, 서 화 정\*\*

## 요 약

소인수분해와 같이 매우 큰 경우의 수를 탐색하고 연산하며 비교하는 작업에서 강점을 가지는 양자컴퓨터는 현재 사용되는 암호체계를 붕괴시킬 수 있다는 점에서 위협이 될 수 있다. 하지만 화학, 머신러닝과 같은 분야에서는 대단히 큰 혁신을 가져올 차세대 컴퓨터로 주목받고 있으며, IBM, Google, Amazon과 같은 세계적인 IT 기업들이 이러한 양자컴퓨터 관련 연구개발에 적극적으로 투자하고 있다. 본 고에서는 양자컴퓨터의 최근 개발 현황과 양자컴퓨팅을 위한 플랫폼인 IBM Qiskit, Google Cirq, ProjectQ, Amazon Braket, Microsoft Azure Quantum, Intel Quantum SDK에 대해 알아보고자 한다.

## I. 서 론

특정한 문제를 효율적으로 모델링하고 해결할 수 있는 양자컴퓨터는 기존의 슈퍼컴퓨터로는 불가능했던 복잡한 연산을 다항 시간 안에 수행할 수 있는 차세대 컴퓨터로 주목받고 있다. 양자컴퓨터는 매우 큰 경우의 수를 탐색하고 연산하며 비교하는 작업에서 강점을 가지는데, 대표적으로 소인수분해가 이러한 작업에 해당된다. 2019년 구글의 양자컴퓨터 연구팀은 2048 비트 자연수를 양자컴퓨터로 소인수분해하는 작업에 대략 8시간이 걸린다고 주장하였다[1]. 물론 해당 작업에 약 2000만개의 큐비트가 필요하므로 실제로 동작하기까지는 많은 시간이 소요될 것으로 예상된다. 하지만 현재 사용되는 암호체계는 1024, 2048 비트의 자연수의 소인수분해가 어렵다는 사실에 기반하고 있으므로 양자컴퓨터의 등장은 이러한 암호를 무력화할 수 있다는 점에서 큰 위협이 된다. 본 고에서는 이러한 양자컴퓨터의 최근 개발 현황과 양자컴퓨팅을 위한 플랫폼 동향에 대해 알아본다.

## II. 양자컴퓨터 소개 및 개발 현황

### 2.1. 양자컴퓨터

양자컴퓨터는 양자 역학의 특성을 활용한 차세대 컴퓨터이다. 큐비트(qubit)는 양자 컴퓨터의 기본 연산 단위로, 초전도 회로(superconducting circuitry), 이온 트랩(trapped ions), 광자(photons) 등 다양한 기술을 통해 만들어진다. 이러한 큐비트는 양자 현상인 얽힘(entanglement)과 중첩(superposition) 성질을 가진다. 큐비트들이 서로 얽혀있는 경우, 어떤 큐비트의 상태가 변화하면 다른 큐비트의 상태에도 영향을 줄 수 있는데 이 성질을 얽힘이라고 한다. 중첩은 0과 1의 상태를 동시에 확률적으로 가질 수 있는 상태를 말한다. 양자컴퓨터는 중첩 성질에 의해  $n$ 개의 큐비트로  $2^n$ 개의 값을 동시에 나타낼 수 있다. 따라서 이러한 양자 역학의 성질을 이용하면 모든 경우의 수에 대해 연산이 순차적으로 수행되는 것이 아니라 동시에 수행되므로 고전컴퓨터에 비해 연산 속도가 획기적으로 빨라지게 된다.

본 연구는 2023년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (<Q|Crypton>, No.2019-0-00033, 미래컴퓨팅 환경에 대비한 계산 복잡도 기반 암호 안전성 검증 기술개발, 50%) 그리고 본 연구는 2023년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥-센터의 지원을 받아 수행된 연구임 (No.2018-0-00264, IoT 융합형 블록체인 플랫폼 보안 원천 기술 연구, 50%).

\* 한성대학교 IT융합공학과 (대학원생, dlatpwls834@gmail.com, khj1594012@gmail.com, dudejrdl123@gmail.com, starj1023@gmail.com, yujin.yang34@gmail.com, oyj0922@gmail.com)

\*\* 한성대학교 융합보안학과 (부교수, hwajeong84@gmail.com)

## 2.2. 양자컴퓨터 개발 현황

### 2.2.1. IBM

초전도 프로세서 기반의 양자컴퓨터를 개발하는 IBM은 2022년 11월 세계 최초로 433 큐비트 양자컴퓨터인 Osprey를 발표했다. IBM은 새로운 시대를 열겠다는 포부를 가지고 [표 1]의 양자 하드웨어 개발 로드맵을 따라 매년 큐비트 목표를 달성한 양자컴퓨터를 공개하고 있으며, 오는 2025년까지 4158 이상의 큐비트를 달성하는 것을 목표로 하고 있다. 올해 공개 예정인 Heron은 지원 큐비트 수가 현저히 줄어든 것에 반해 고품질의 큐비트를 가지며, 각각의 칩을 다른 Heron 프로세서에 직접 연결하는 기술을 통해 구현된다. 이를 통해 단일 칩 상에서 지원하는 큐비트 수를 늘렸던 지금까지 양자 하드웨어와는 달리 다수의 프로세서가 연결된 모듈형 양자컴퓨터로 개발 방향이 전환된다는 것을 알 수 있다. 이는 큐비트 규모를 확장하기 위한 IBM의 해결책이다.

양자컴퓨터의 성능은 큐비트 수로만 평가하기 어렵다. 따라서 IBM은 양자컴퓨터의 능력을 측정하기 위한 지표로 양자 볼륨(quantum volume)을 제시하였다. 양자 볼륨은 실행할 수 있는 양자 회로의 크기를 나타내며, 양자컴퓨터의 효율성을 표현한 매트릭으로 볼 수 있다. 양자 볼륨은 큐비트 수, 오류율 및 큐비트의 연결성을 고려하여 계산되는데 여기서 큐비트 수는 물리적인 큐비트 수를 말하며, 오류율은 양자 연산에 존재하는 오류를 말한다. 큐비트의 연결성은 큐비트 간의 얽힘 성질을 의미하여 이 요소가 세 가지 요소 중 양자 볼륨을 결정하는 핵심 요소가 된다. 2022년 27 큐비트 Falcon 계열의 Prague 양자컴퓨터에서 512의 양자 볼륨을 달성했다. 이는 9 큐비트와 회로 깊이 9를 가지는 양자 회로를 성공적으로 실행했음을 의미한다[3].

[표 1] IBM 양자 하드웨어 개발 로드맵(2)

Year	2019	2020	2021	2022	2023		2024		2025	2026
Processor	Falcon	Hummingbird	Eagle	Osprey	Condor	Heron	Flamingo	Crossbill	Kookaburra	-
Qubit	27	65	127	433	1,121	133	1,386+	408	4,158+	10K ~ 100K

### 2.2.2. Google

Google도 IBM과 마찬가지로 초전도 기반의 양자 프로세서를 개발하고 있다. 2019년 10월 오류율을 대폭 낮춰 실제로 프로그래밍이 가능한 54 큐비트의 Sycamore를 발표했으며, 단순 양자 자원 측면의 성과가 아닌 실제로 동작 가능한 프로세서라는 점에서 의미가 있다. 또한 같은 시기에 Sycamore는 세계에서 가장 빠른 슈퍼컴퓨터인 Summit으로 10,000년이 걸리는 난수 증명 작업을 200초 만에 수행함으로써 세계 최초로 양자 우위를 달성하였다[4]. Google의 양자컴퓨터 실용성 검증은 양자컴퓨터의 실현 가능성에 의문을 제기하던 연구자들이 앞으로 다가올 양자컴퓨터 시대를 위한 연구에 집중할 수 있는 토대가 된 유의미한 결과로 볼 수 있다. Google은 현재 오류율을 최소화하여 운영할 수 있는 프로세서 개발에 집중하고 있으며 향후 2029년까지 유용한 양자컴퓨터 개발 및 1,000,000 큐비트 달성을 목표로 하고 있다.

### 2.2.3. IonQ

IonQ는 Amazon, Microsoft와 기아, 현대차에서 투자 중인 양자컴퓨터 스타트업 회사이다. 현재 Amazon Braket, Microsoft Azure Quantum, Google 클라우드 서비스를 통해 IonQ의 양자컴퓨터를 제공하고 있다. 이온트랩 기반의 양자컴퓨터를 제공하는데, 이온트랩은 자연적으로 발생하는 양자시스템인 원자를 큐비트로 사용한다. IonQ의 큐비트로 사용되는 원자는 이온화된 상태이며, 안정적인 상태의 양자가 준비되면 오랫동안 상태를 유지할 수 있는 특징을 가진다. 원자를 이온상태로 바꾼 큐비트를 다루기 위해 이온트랩을 사용한다. 이온트랩 기반의 양자 프로세서는 큐비트는 품질이 좋다는 특징을 가진다. 큐비트의 높은 품질은 큐비트 간 연결성이 좋고 게이트 에러율이 낮기 때문에 큐비트 수가 적더라도 우수한 성능을 보인다. 2022년 현재 32 큐비트급의 양자컴퓨터 Aria를 클라우드

서비스로 제공하고 있다[5].

### III. 양자컴퓨터 플랫폼 동향

양자컴퓨팅을 위한 플랫폼은 IBM Qiskit, Google Cirq, ProjectQ, Amazon Braket, Microsoft Azure Quantum, Intel Quantum SDK 등이 있으며, 각 플랫폼은 양자 응용 프로그램을 구현하고 실행할 수 있도록 다양한 기능과 시뮬레이터 및 하드웨어를 제공한다. 본 장에서는 각 플랫폼에 대해 상세히 알아본다.

#### 3.1. IBM Qiskit[6]

Qiskit은 IBM에서 개발한 오픈소스 양자 소프트웨어 프레임워크이며, Quantum Lab과 Quantum Composer 기능을 제공한다. Quantum Lab을 사용하면 Jupyter notebook 형식으로 Python과 OpenQASM(Open Quantum Assembly Language)를 활용하여 구현이 가능하고, Composer 기능을 사용하면 드래그 앤 드롭(Drag and drop) 방식을 통해 큐비트 및 양자 게이트를 배치할 수 있어 보다 쉽게 회로를 구성하고 실행할 수 있다. 또한 Composer에서 제공하는 시각화 기능을 통해 실행된 회로의 결과에 대한 확률과 블로흐 구의 상태 및 상태 벡터를 확인할 수 있다. 이러한 양자 회로 구성과 관련된 기능은 Qiskit이 다른 플랫폼에 비해 우수하다고 평가받아 현재 양자컴퓨팅 플랫폼 중 가장 높은 인지도를 차지하고 있다. 또한 IBM에서는 이러한 플랫폼의 활성화를 위해 매년 해커톤과 Quantum Open Science Prize를 개최하고 있으며, slack 채널을 통해 정보 공유와 문제 해결이 활발히 이루어지고 있다.

Qiskit은 양자 프로그램의 실행을 위해 시뮬레이터와 자사의 실제 하드웨어를 제공한다. 양자 시뮬레이터는 양자컴퓨터에서 수행하는 연산을 고전컴퓨터에서 수행하는 것이며, 목적에 따라 사용할 수 있도록 다양한 시뮬레이터를 제공하고 있다. 그 중 qasm 시뮬레이터는 하드웨어에서 작동하는 방식과 유사하며 Shots 수에 따라 확률이 결정된다. 즉 100번 중 90번의 측정 결과가 0인 경우에 측정 확률은 (0.9, 0.1)이다. 또한 고품질의 노이즈 모델링을 지원하며 다양한 회전 게이트를 사용할 수 있다. statevector 시뮬레이터는 큐비트의 상태 벡터를 관찰할 수 있는 시뮬레이터로,  $n$  큐비

[표 2] Qiskit의 시뮬레이터에 따른 큐비트별 회로 실행시간 (단위: 초)

Qubit	10	20	28	29
qasm	0.047	0.085	4.144	Dead
Qubit	10	20	24	25
statevector	0.395	119.092	2319.701	Dead

트에 대해  $2^n$  길이의 상태 벡터를 반환하는데 이 과정에서 qasm 시뮬레이터보다 더 많은 시간과 메모리가 요구된다. 또한 일반 노이즈 모델링을 지원하며 다양한 회전 게이트를 사용할 수 있다. [표 2]는 두 시뮬레이터에 대한 큐비트 개수별 실행시간을 보여준다. 사용된 회로는 X 게이트로 구성되었으며, 30의 회로 깊이를 가지며 회로 반복 횟수인 shots은 1024로 설정하였다. 또한, 본 고에서 수행한 시뮬레이터 및 하드웨어 성능 평가에는 해당 양자 회로 구조가 사용되었다. 두 시뮬레이터 모두 32 큐비트를 지원한다는 Qiskit 공식 문서와는 다르게 실제로 측정했을 때는 큐비트 수가 늘어남에 따라 연산 시간이 급격히 증가하였으며, qasm 및 statevector 시뮬레이터는 각각 최대 28 큐비트, 24 큐비트까지만 동작 가능하였다.

Qiskit은 IBM의 실제 하드웨어에 접근할 수 있도록 하며, 현재 Osprey 프로세서를 사용하는 433 큐비트의 하드웨어까지 존재한다. 하지만 일반 사용자는 최대 7 큐비트의 하드웨어까지만 무료로 사용할 수 있다. 기존에는 7 큐비트 이상의 하드웨어를 사용하기 위해 연구자 등록 절차가 요구되었지만 최근에는 ‘pay-as-you-go’ 방식을 통해 유료로 27 큐비트까지 사용할 수 있게 되었다. 해당 프로세서는 2개의 Falcon 프로세서이며, 최대 8시간 사용이 가능하다. Qiskit에서 하드웨어를 사용하기 위해서는 회로를 구성한 뒤 원하는 하드웨어를 백엔드로 설정하면 된다. 프로그램 실행은 동작 대상 회로가 대기 큐(Queue)에 입력된 후, 하드웨어가 배정되면 실행되는 방식이다. [표 3]은 IBM의 ‘ibmq\_manila’와 ‘ibmq\_nairobi’ 하드웨어를 사용하여 측정한 큐비트별 실행시간을 나타

[표 3] Qiskit의 하드웨어에 따른 큐비트별 회로 실행시간 (단위: 초)

Qubit	3	5
ibmq_manila	5.6	6.0
Qubit	3	7
ibmq_nairobi	9.1	51.2

낸다. 실행시간은 큐에서 대기한 시간을 제외하고 회로 동작시간만을 측정할 결과이다. Qiskit 공식 자료에 명시된 내용과 동일하게 각각 5 큐비트, 7 큐비트까지 사용 가능한 것을 확인하였다. 이외에도 Qiskit은 실제 하드웨어는 아니지만 IBM의 실제 하드웨어 동작 방식을 모방하도록 구축된 fake hardware도 제공한다. fake hardware는 노이즈 시뮬레이션을 제공하고 5~127 큐비트의 백엔드를 사용할 수 있지만, 실행속도가 매우 느리다는 단점이 있다.

### 3.2. Google Cirq[7]

Google Quantum AI에서 제공하는 Cirq는 노이즈가 많은 중간 규모의 양자인 NISQ(Noisy Intermediate Scale Quantum) 장치용 양자 알고리즘을 작성하기 위한 오픈소스 프레임워크이다. 여기서 NISQ 장치는  $O(1000)$  게이트를 실행할 수 있는  $O(100)$  큐비트가 있는 장치를 의미한다. Cirq의 Moment라는 개념을 통해 다양한 삽입 기능을 구현할 수 있으며 이를 활용하여 원하는 회로를 구축할 수 있다. Python 기반으로 동작하며,

Cirq에는 작은 회로를 테스트하기 위한 파동함수 및 밀도 매트릭스용 Python 시뮬레이터가 내장되어있다. 각각 ‘Simulator’, ‘DensityMatrixSimulator’이며, 두 시뮬레이터는 모두 노이즈가 있는 양자 채널에 대해 수행할 수 있다. 또한 Cirq는 C++로 작성된 최첨단 파동함수 시뮬레이터인 qsim과 함께 작동한다. 내장된 시뮬레이터를 사용하면 약 20큐비트까지 사용이 가능하지만, qsim은 사용할 수 있는 큐비트 수를 높여 90 코어의 Intel Xeon 워크스테이션에서 최대 40 큐비트까지 시뮬레이션이 가능하다. 이러한 시뮬레이터들은 Quantum Virtual Machine으로 양자 하드웨어를 모방하는데 사용될 수 있다. [표 4]는 Cirq에 내장된 기본 시뮬레이터를 사용했을 때의 큐비트별 회로 실행시간이며, 최대 30 큐비트까지 동작 가능함을 확인하였다.

[표 4] Cirq의 기본 시뮬레이터에 대한 큐비트별 회로 실행시간

(단위: 초)

Qubit	10	20	30
Simulator	0.009	0.05	274.29

### 3.3. ProjectQ[8]

취리히 공과대학교 연구팀에서 양자컴퓨팅을 위해 개발된 오픈소스 소프트웨어 프레임워크인 ProjectQ는 Python 기반으로 동작하며, ProjectQ에서 제공하는 라이브러리를 통해 다양한 양자 프로그램을 구현할 수 있다. 또한 시뮬레이터, 에뮬레이터, 실제 하드웨어와 같은 여러 가지 유형의 백엔드를 사용하여 실행할 수 있으며, 각각의 백엔드는 다양한 기능을 제공한다. Main engine에서 사용하는 기본 시뮬레이터인 ‘Simulator’는 C++를 기반으로 하여 빠른 속도를 가진다는 특징이 있으며 사용 가능한 큐비트가 제한되어 있다. Hadamard, T 게이트 등은 사용할 수 없고 고전적인 작업만 허용하는 ‘ClassicalSimulator’는 수만 개의 큐비트까지 동작 가능하다. 또한 양자 회로에 사용된 큐비트 수, 게이트 수 등과 같은 양자 자원을 추정하는 백엔드인 ‘Resource counter’ 등이 있다. 이외에도 Amazon Braket, Azure Quantum, IBM Qiskit, IonQ 등의 디바이스를 지원하기 위한 백엔드들이 존재한다. [표 5]는 Main engine의 기본 시뮬레이터를 사용할 때의 큐비트별 회로 실행시간이며, 최대 31 큐비트까지 동작이 가능한 것을 확인하였다.

[표 5] ProjectQ의 기본 시뮬레이터에 대한 큐비트별 회로 실행시간

(단위: 초)

Qubit	10	20	30	31
Simulator	0.205	0.242	119.815	319.266

### 3.4. Amazon Braket[9]

Braket은 양자컴퓨팅을 위해 Amazon에서 개발한 클라우드 서비스이다. Braket 클라우드 서비스를 통해 양자 알고리즘을 설계하고 양자 시뮬레이션을 수행할 수 있으며 양자 하드웨어를 제공하는 업체의 양자 자원과 기술을 사용할 수 있도록 제공한다. 제공되는 양자 하드웨어에는 게이트 기반 초전도 프로세서, 이온 트랩 프로세서, 중성 원자 기반 양자 프로세서 등과 같이 다양한 종류가 있다. 또한 Notebook에서 인스턴스를 생성하여 Jupyter notebook 형식으로 개발할 수 있으며, Python과 OpenQASM을 활용하여 양자 프로그램을 구현할 수 있다. 일부 서비스는 매일 1시간 이내

[표 6] Braket 시뮬레이터의 큐비트별 회로 실행시간

(단위: 초)

Qubit	10	20	25
Local	0.02	0.48	22.86

무료 시뮬레이션이 가능하고 Research 프로그램에 선 발된 사용자의 경우 AWS 서비스를 무료로 사용할 수 있다. 또한 양자 하드웨어 제공에 대한 업데이트가 활발이 이루어지고 있다.

구현된 양자 프로그램은 Braket에서 제공하는 시뮬레이터 및 하드웨어를 사용하여 동작시킬 수 있다. Braket은 무료인 ‘Local’ 시뮬레이터와 유료인 ‘State Vector(SV1)’, ‘Density Matrix(DM1)’, ‘Tensor Network(TN1)’ 총 4가지 시뮬레이터를 제공한다. 모든 시뮬레이터의 로컬 실행 시 최대 런타임 시간은 6 시간이다. ‘Local’과 ‘SV1’은 상태 벡터를 시뮬레이션 하고 범용적인 양자 회로를 지원하며, 각각 최대 25 큐비트, 34 큐비트까지 동작시킬 수 있다. 또한 실제 양자컴퓨터처럼 노이즈 시뮬레이션이 가능한 ‘DM1’ 시뮬레이터, 양자 푸리에 변환과 같이 규칙성이 있는 회로 시뮬레이션 및 대규모 시뮬레이션에 특화된 ‘TN1’ 시뮬레이터를 제공한다. 각각 최대 17 큐비트, 50 큐비트까지 동작시킬 수 있다. [표 6]은 ‘Local’ 시뮬레이터에 대한 큐비트별 회로 실행시간을 보여주며, 최대 큐비트인 25 큐비트까지 동작 가능한 것을 확인하였다.

### 3.5. Microsoft Azure Quantum[10]

Azure Quantum은 Microsoft에서 2021년 출시한 클라우드 양자컴퓨팅 서비스로, 자사에서 제공하는 양자 프로그램 개발 도구인 Quantum Development Kit(QDK)를 통해 Jupyter notebook 형식의 Azure Quantum 서비스를 사용할 수 있다. 기본적으로 Python과 QDK에 포함된 양자 프로그래밍 언어인 Q#을 사용하여 작성할 수 있으며, 가장 많이 사용되는 양자 SDK인 IBM의 Qiskit과 Google의 Cirq도 지원하므로 개발 도구의 다양성을 보장해준다. 또한 Azure Protal을 이용하거나 QDK로 자체 로컬 개발 환경을 설정하는 방법을 통하여 양자 프로그램을 생성하고 실행할 수 있다. Azure Quantum 서비스를 사용하면 이온 트랩 방식의 IonQ, Quantinuum과 초전도체 방식의 QCI, Rigetti를 포함한 8개의 공급자가 제공하는

[표 7] Azure Quantum의 디바이스에 따른 큐비트별 회로 실행시간

(단위: 초)

Qubit	10	18	19
ionq.simulator	20.07	22.8	Error
Qubit	5		
ionq.qpu	Dead		

디바이스 상에서도 동작이 가능하다. 그 중, IonQ의 디바이스에 접근하여 성능을 측정하였으며, [표 7]은 그 결과를 나타낸다. 현재 접근할 수 있는 디바이스를 기준으로 IonQ의 시뮬레이터와 하드웨어는 각각 29, 23 큐비트를 제공한다. IonQ에서 제공하는 시뮬레이터의 경우, 최대 29 큐비트까지 지원한다는 공식 문서와 달리 실제 측정한 결과 19 큐비트에서 에러가 발생하였다. 하드웨어의 경우, 23 큐비트까지 지원한다는 ‘ionq.qpu.aria-1’은 5 큐비트를 할당한 경우에도 최대 런타임 시간을 초과했으며, 11 큐비트까지 지원하는 ‘ionq.qpu’도 동일하게 5 큐비트 할당 시 런타임 시간을 초과하였다. 양자 하드웨어의 경우 시스템이 불안정한 상태로 사료된다.

Azure Quantum은 신규 및 학생 회원에게는 무료 사용을 위한 크레딧을 제공해주고 실행시간 등에 따른 요금을 부과한다. 또한 QRNG와 Grover search 등 다양한 샘플 코드 및 커스텀 모델 작성을 위한 튜토리얼을 제공한다.

### 3.6. Intel Quantum SDK[11]

올해 2월 Intel은 Quantum 소프트웨어 개발 키트(SDK) 버전 1.0을 출시했다. 업계 표준 LLVM(Low Level Virtual Machine) 컴파일러를 사용하여 C++로 작성된 직관적인 프로그래밍 인터페이스를 가지는 것이 특징이다. 개발자들이 오랫동안 사용해온 C++을 사용하여 양자 알고리즘을 구축할 수 있기 때문에 양자컴퓨팅 개발 경험이 전무한 사람도 쉽게 접근하여 작업할 수 있다. Intel의 SDK는 C, C++ 및 Python 응용 프로그램과의 원활한 인터페이스도 제공한다. 또한 하이브리드 양자-고전 알고리즘 실행에 최적화된 양자 런타임 환경을 제공한다. 개발자는 2개의 백엔드를 선택할 수 있는데, 고성능 오픈 소스 일반 큐비트 시뮬레이터인 Intel Quantum Simulator(IQS)와 Intel Quantum Dot 큐비트 하드웨어를 시뮬레이션하고

Intel의 실리콘 스핀 큐비트의 소형 모델 시뮬레이션을 가능하게 하는 백엔드가 있다. Intel의 큐비트는 실리콘 트랜지스터 기반이다. Intel Quantum SDK 1.0은 현재 OneAPI Intel Dev Cloud에서 사용할 수 있으며, 액세스 권한을 허가 받은 후 사용이 가능하다. 단일 계산 노드에서 최대 32 큐비트를, 여러 노드에서 40 큐비트 이상의 애플리케이션 및 알고리즘을 시뮬레이션할 수 있는 실행 파일 구축이 가능하다.

#### IV. 결 론

양자컴퓨터는 고속 연산 능력을 기반으로 여러 난제를 해결할 수 있어 현재 산업의 판도를 바꿀 것으로 주목받고 있다. IBM, Google 등 세계적인 IT 기업이 양자컴퓨터 산업에 큰 관심을 가지고 연구개발이 수행되고 있다. 또한 다양한 양자컴퓨팅 플랫폼들이 등장하고 있으며, 양자컴퓨터 활용을 위한 다양한 서비스 및 라이브러리를 제공하고 있다. 또한 양자 플랫폼을 제공하는 기업이 자체적인 양자컴퓨터를 개발하지 않더라도 이를 개발하는 양자 하드웨어 업체의 기술과 자원을 호환하여 사용할 수 있도록 지원하고 있다. 이를 통해 양자컴퓨터 산업이 유연하게 개발되고 있음을 알 수 있으며, 이러한 플랫폼을 활용하면 양자컴퓨팅 기술을 응용한 여러 산업이 빠르게 발전할 수 있을 것으로 기대할 수 있다.

#### 참 고 문 헌

- [1] Craig Gidney and Martin Ekerå, “How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits,” <https://arxiv.org/abs/1905.09749>, 2019
- [2] The IBM Quantum Development Roadmap[Website]. (2023, Mar 29). <https://www.ibm.com/quantum/roadmap>.
- [3] The 2022 IBM Research annual letter[Website]. (2023, Mar 29). <https://research.ibm.com/blog/research-annual-letter-2022>.
- [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] IonQ Aria[Website]. (2023, Mar 29). <https://ionq.com/quantum-systems/aria.z>
- [6] Qiskit Runtime[Website]. (2023, Mar 29). <https://www.ibm.com/quantum/qiskit-runtime>.
- [7] Introduction to Cirq[Website]. (2023, Mar 29). <https://quantumai.google/cirq/start/intro>.
- [8] Steiger, Damian S., Thomas Häner, and Matthias Troyer. “ProjectQ: an open source software framework for quantum computing,” *Quantum* Vol. 2, pp. 49, 2018.
- [9] Amazon Braket[Website]. (2023, Mar 29). <https://aws.amazon.com/ko/braket/>.
- [10] Azure Quantum[Website]. (2023, Mar 29). <https://azure.microsoft.com/ko-kr/products/quantum>
- [11] Wu, Xin-Chuan, et al. “Intel Quantum SDK Version 1.0: Extended C++ Compiler, Runtime and Quantum Hardware Simulators for Hybrid Quantum-Classical Applications,” *Bulletin of the American Physical Society*, 2023.

#### < 저 자 소 개 >



임 세 진 (SeJin Lim)

학생회원

2022년 2월 : 한성대학교 컴퓨터공학부 졸업

2022년 3월~현재 : 한성대학교 IT융합공학과 석사과정

<관심분야> 양자컴퓨터, 인공지능 보안, 정보보안



김 현 지 (Hyunji Kim)

학생회원

2020년 2월 : 한성대학교 IT응용시스템공학과 졸업

2020년 3월~2022년 2월 : 한성대학교 IT융합공학과 석사 졸업

2022년 3월~현재 : 한성대학교 정보컴퓨터공학과 박사과정

<관심분야> 정보보안, 인공지능, 양자 컴퓨팅



**김 덕 영 (Dukyoung Kim)**

2019년 2월 : 한성대학교 디자인 아트  
평생교육원 인테리어디자인과 졸업  
2023년 3월~현재 : 한성대학교 융합  
보안학과 석사과정  
<관심분야> 정보보안, 인공지능



**오 유 진 (Yujin Oh)**

학생회원  
2023년 2월 : 한성대학교 IT융합공학  
부 졸업  
2023년 3월~현재 : 한성대학교 융합  
보안학과 석사과정  
<관심분야> 양자컴퓨터, 암호구현



**장 경 배 (Kyungbae Jang)**

학생회원  
2019년 2월 : 한성대학교 IT응용시스  
템공학과 공학 학사  
2021년 2월 : 한성대학교 IT융합공학  
과 석사과정  
2021년 3월~현재 : 한성대학교 정보  
컴퓨터공학과 박사과정

<관심분야> 양자컴퓨터, 정보보안



**서 화 정 (Hwajeong Seo)**

증신회원  
2010년 2월 : 부산대학교 컴퓨터공학  
과 졸업  
2012년 2월 : 부산대학교 컴퓨터공학  
과 석사  
2016년 1월 : 부산대학교 컴퓨터공학  
과 박사

2016년 1월~2017년 3월 : 싱가포르 과학기술청  
2017년 4월~2023년 2월 : 한성대학교 IT융합공학부 조교수  
2023년 2월~현재 : 한성대학교 융합보안학과 부교수  
<관심분야> 정보보안, 암호구현



**양 유 진 (Yujin Yang)**

학생회원  
2022년 2월 : 한성대학교 IT융합공학  
부 졸업  
2022년 3월~현재 : 한성대학교 IT융  
합공학과 석사과정  
<관심분야> 양자컴퓨터, 정보보안