Chapter
03

안전한 양자 컴퓨팅 사용을 위한 양자 데이터 암호화 기술 동향

김주영_한국전자통신연구원 선임연구원

양자 컴퓨팅은 당분간 클라우드 기반 위임 사용 모델이 중심이 될 가능성이 크다. 이 과정에서 입력 상태, 회로 구조, 파라미터, 결과값을 보호하기 위한 보안 기술이 필요하며, 대표적 기반 기술로는 파울리 프레임 기반 양자 원타임 패드가 있다. 클리포드 게이트는 비교적 효율적으로 처리되지만, 비클리포드 게이트는 추가 자원과 보정 절차를 요구하여 실용화의 병목으로 작용한다. 최근에는 양자 동형암호 실험, 검증 기술, 동적 회로 지원, 표준화와 상호운용성 논의가 함께 발전하고 있다. 결국, 안전한 양자 클라우드는 보안 기법 뿐 아니라 이를 구현·운영할 시스템 기능과 표준 생태계가 함께 갖춰질 때 실용화될 수 있다.

I. 서론

최근 양자 컴퓨팅 기술이 급격히 발전함에 따라 신약 개발, 신소재 발굴, 복잡한 최적화 문제 해결 등 다양한 산업 및 연구 분야에서 양자 컴퓨팅의 필요성이 대두되고 있다. 그러나 현재의 양자 컴퓨터는 물리적 구현, 큐비트의 오류 보정 그리고 극저온 환경 유지 등에 막대한 비용과 고도의 인프라가 요구된다[1].

따라서 양자 컴퓨팅 기술의 초기 상용화 모델은 과거 초기 디지털 컴퓨터나 현재의 클라우드 컴퓨팅 아키텍처와 유사한 형태를 띨 것으로 전망된다. 즉, 모든 사용자가 자체적인 고성능 양자 컴퓨터를 소유하는 대신, 소수의 기업이나 국가 기관이 구축한 대규모 양자 인프라에 접속하여 복잡한 연산을 위탁하는 양자 클라우드 기반의 서비스 모델이 주를 이룰 것이다.

* 본 내용은 김주영 선임연구원(☎ 042-860-0916, ap424@etri.re.kr)에게 문의하시기 바랍니다.
** 본 내용은 필자의 주관적인 의견이며 IITP의 공식적인 입장이 아님을 밝힙니다.
***이 보고서는 한국전자통신연구원 연구운영비지원사업 (26ZS1320,데이터 프라이버시 완벽 보장을 위한 양자 기반 新암호체계 원천 기술 연구)의 지원을 받아 작성된 보고서입니다.

양자 클라우드 환경은 구조적으로 클라이언트-서버 구조를 가진다. 제한적인 양자 자원을 보유하거나 약한 연산 능력만을 갖춘 클라이언트(사용자)는 대규모 양자 회로 구동 및 복잡한 연산 처리가 가능한 고성능 양자 서버에 자신의 연산을 위임해야 한다. 이러한 위임형 컴퓨팅 구조는 양자 컴퓨팅의 접근성을 높이고 자원 활용성을 높이는 주요 수단이 된다.

그러나 이 같은 연산 위탁 구조는 구조적인 보안 취약점을 가지고 있다. 연산을 위탁받는 양자 클라우드 서버가 보안 측면에서 완벽히 신뢰할 수 없는 환경일 경우, 서버 관리자나 악의적인 공격자에 의해 보안 사고가 발생할 수 있다.

기존의 고전 컴퓨팅 환경과 달리 양자 컴퓨팅 환경에서는 위탁 연산 수행 과정 중 사용자의 고유한 양자 알고리즘, 민감한 입력 데이터 그리고 최종 연산 결과값 등 핵심적인 양자 상태 데이터가 서버에 그대로 노출될 위험이 존재한다.

결과적으로, 양자 컴퓨터의 잠재적 계산 이점을 안전하게 활용하기 위해서는 클라이언트와 서버 간의 데이터 송수신뿐만 아니라, 연산이 수행되는 과정 자체에서도 데이터의 기밀성과 무결성을 보장할 수 있는 새로운 보안 접근 방식이 요구된다.

이에 따라, 양자 상태의 데이터를 안전하게 보호하면서도 서버 측에서 큐비트 연산을 수행할 수 있도록 지원하는 차세대 양자 암호 기술이 주요 접근법으로 주목받고 있다. 이들 기술은 정보 이론적 보안을 기반으로 하고, 범용 회로로의 확장이나 결과 검증 단계에서는 계산적 가정과 결합하기도 한다.

본 고에서는 신뢰할 수 없는 양자 환경에서도 데이터 노출 가능성을 낮출 수 있는 양자 암호화 메커니즘의 기술적 동향을 분석하고, 안전한 양자 컴퓨팅 환경 구축을 위한 시사점을 도출한다.

II. 양자 연산 위탁을 위한 핵심 보안 원리와 기반 기술

클라우드 기반의 양자 컴퓨팅 환경에서는 연산 능력이 제한적인 클라이언트가 복잡한 양자 회로의 실행을 강력한 양자 자원을 보유한 서버에 위임한다. 이때 서버를 완전히 신뢰할 수 없다면, 클라이언트의 민감 정보가 유출될 수 있는 다양한 노출면이 존재한다.

구체적으로 입력되는 양자 데이터 상태뿐만 아니라, 사용자가 실행하고자 하는 양자 회로의 구조, 게이트의 종류, 알고리즘 구동을 위한 최적화 파라미터 자체가 보호해야 할 대상이

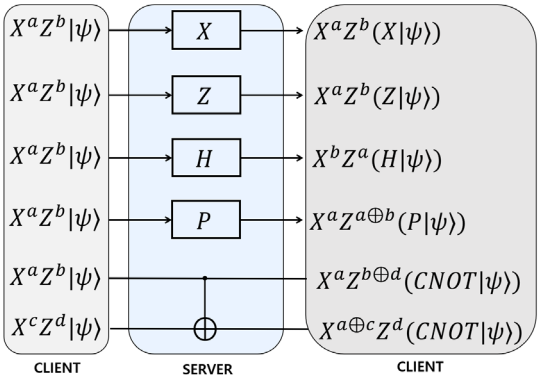
된다. 따라서 클라이언트-서버 간 통신 구간의 암호화를 넘어, 큐비트가 서버의 메모리에 적재되어 연산이 수행되는 전 과정에서 양자 상태를 은닉하는 사용 중인 데이터 보호 기술이 필수적으로 요구된다[2][3].

양자 연산 위탁 환경에서 기밀성을 보장하는 가장 근본적인 접근법은 양자 원타임 패드를 이용한 상태 마스킹이다. 고전적인 일회용 암호가 평문 비트에 무작위 키를 XOR 연산하여 암호화하듯이 양자 원타임 패드에서는 단일 큐비트 상태 $|\psi\rangle$ 에 대해 클라이언트가 무작위 고전 비트 키 $a,b\in\{0,1\}$를 생성하고 파울리 연산자 X^aZ^b를 적용하여 암호화된 상태 ρ_{enc}를 생성한다[4].

이 과정을 거친 큐비트의 밀도 행렬(density matrix)은 최대 혼합 상태(maximally mixed state)가 되며, 이는 키를 모르는 서버 입장에서 해당 큐비트가 어떤 상태인지 정보 이론적으로 전혀 알 수 없다[4].

클라이언트는 데이터를 서버로 전송하기 전 이와 같이 각 큐비트에 무작위 파울리 연산을 가하여 마스킹하며, 서버는 암호화된 상태 그대로 양자 회로를 구동한다. 연산이 종료된 후 반환된 결과 큐비트는 클라이언트가 자신이 보유한 파울리 키를 역으로 적용하여 복호화함으로써 안전하게 최종 측정값을 획득한다[4].

서버가 암호화된 큐비트 위에서 논리적 게이트를 수행하기 위해서는, 마스킹된 상태를 풀지 않고도 연산 결과가 유효하게 누적되어야 한다. 이를 해결하는 핵심 메커니즘이 파울리



〈자료〉 K. A. G. Fisher et al., “Quantum computing on encrypted data”, Nature Communications, Vol.5, Article 3074, 2014(doi:10.1038/ncomms4074). 재구성

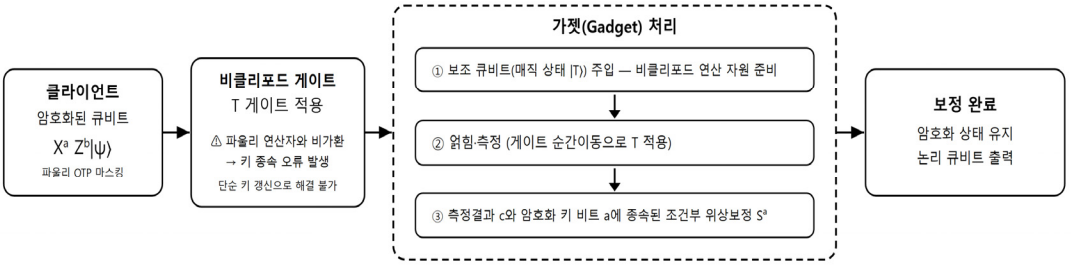
[그림 1] 파울리 프레임 기반 암호화 위임 연산 개념 및 클리포드 게이트에서의 키 갱신 구조

프레임 갱신이다. 하지만 적용되는 양자 게이트의 수학적 특성에 따라 처리 방식과 소모되는 자원의 오버헤드가 크게 달라진다[5][6]. 클리포드 그룹 게이트의 경우, X, Z, H, S, CNOT 등으로 구성되어 임의의 파울리 연산자를 켤레 변환을 통해 다른 파울리 연산자로 변환하는 성질을 가진다. 서버가 암호화된 큐비트에 클리포드 게이트를 적용하면, 물리적인 양자 상태의 오류 누적 없이 클라이언트가 자신의 고전 컴퓨터 상에서 파울리 키 정보만 규칙에 따라 업데이트하는 것만으로 안전하게 연산을 수행할 수 있다. 이와 같은 파울리 프레임 기반 암호화 위임 연산의 전체 구조와 클리포드 게이트에서의 키 갱신 과정은 [그림 1]과 같다.

반면, 비클리포드 그룹 게이트는 보편적 양자 컴퓨팅을 위해 필수적인 T 게이트나 임의의 각도 회전 $R_Z(\theta)$ 연산을 포함한다. 그러나 이 연산들은 파울리 연산자와 단순히 교환되지 않으며, 암호화 키에 종속적인 부가적인 파울리 오류를 발생시킨다.

이를 처리하기 위해, 블라인드 위임 계산 계열은 상호작용을 요구하는 경우가 많고, 양자 동형암호 계열은 비상호작용형도 가능하지만 비클리포드 처리 시 매직 상태 주입과 같은 복잡한 가젯 회로를 구성해야 한다. 비클리포드 게이트를 처리하기 위한 매직 상태 주입 기반 가젯의 개념적 구성은 [그림 2]와 같다.

결론적으로, 비클리포드 연산 처리는 양자 상태의 기밀성을 유지하기 위해 추가 자원과 보정 절차가 필요하며, 이에 따라 얽힘 자원 소모와 통신 오버헤드가 증가한다. 향후 위임형 양자 클라우드 서비스가 실용화되기 위해서는 정보 보안 수준을 유지하면서 이 오버헤드를 최소화할 수 있는 하이브리드 프로토콜 설계와 효율적인 양자 회로 컴파일 기술이 원천 보안 기술의 핵심 과제로 남아 있다[5][6].



〈자료〉 K. A. G. Fisher et al., “Quantum computing on encrypted data”, Nature Communications, Vol.5, Article 3074, 2014(doi:10.1038/ncomms4074). 재구성

[그림 2] 파울리 프레임 암호화 상태에서 비클리포드 게이트(T 계열)를 처리하는 가젯 개념도

III. 안전한 양자 클라우드 구현을 위한 기술 연구 동향

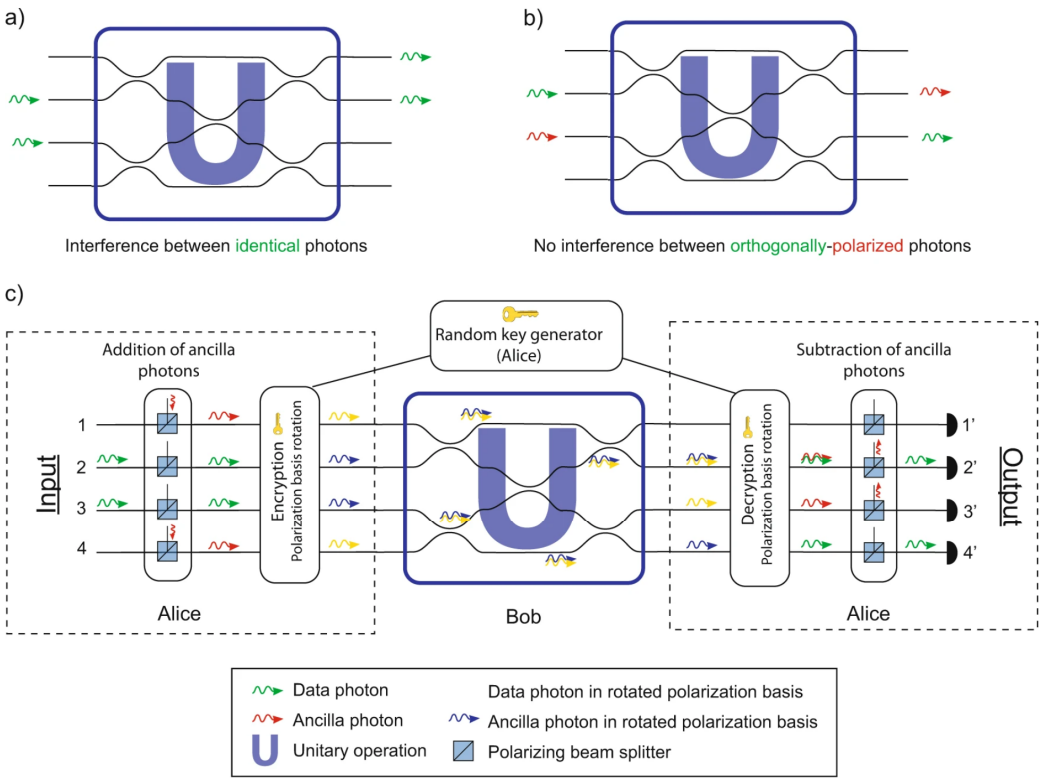
양자 클라우드는 고가의 양자 하드웨어를 소수의 사업자가 집중적으로 구축하고 다수의 사용자가 원격으로 연산을 위탁하는 구조로 확산되고 있다. 이 구조에서 보안 기술 개발의 목표는 서버가 연산을 수행하더라도 사용자의 입력 상태와 결과 그리고 연산 과정에서 드러나는 부가 정보가 불필요하게 노출되지 않도록 하는 기밀성 확보와 서버가 정해진 연산을 수행했는지 및 결과가 조작되거나 훼손되지 않았는지를 확인할 수 있는 무결성 · 검증 가능성 확보로 정리된다. 최근 연구 동향은 파울리 프레임 기반 상태 마스킹을 기본층으로 두고, 암호화된 상태 위에서의 연산 방법, 결과 검증 방법 그리고 이를 가능하게 하는 클라우드 런타임 기능을 함께 발전시키는 방향으로 전개되고 있다.

기밀성 확보의 출발점은 양자 상태를 직접 마스킹하는 양자 원타임 패드이며, 각 큐비트에 무작위 파울리 연산을 적용해 서버 관점에서 상태 정보가 드러나지 않도록 만드는 접근이 제시되었다[4]. 다만, 클라우드 환경에서 실제 구현의 핵심은 마스킹 자체보다도 연산 과정에서 키가 어떻게 변하는지를 정확히 추적하고 반영하는 파울리 프레임 관리에 있다. 이 기능은 보안 프로토콜을 위한 보조 기능을 넘어 오류 보정 및 결함 허용 운영에서의 필수 런타임 기능과 결합되고 있다.

암호화된 상태 위에서의 연산을 본격적으로 다루는 축은 양자 동형암호 계열이다. 양자 동형암호는 클라이언트가 암호화한 양자 데이터를 서버가 복호화 없이 처리하고, 그 결과를 클라이언트가 복호화해 얻는 방식이다. 이때 클리포드 게이트는 파울리 마스킹과의 교환 관계를 통해 키만 갱신하면 되므로 비교적 자연스럽게 처리된다. 반면, 비클리포드 게이트는 파울리 키에 의존하는 추가 보정이 발생해 단순 키 갱신만으로는 해결되지 않으며, 결과적으로 비클리포드 처리 방법이 양자 동형암호의 오버헤드와 실용성을 좌우한다. Broadbent-Jeffery는 T 게이트 복잡도가 낮은 회로에서의 양자 동형암호를 정식화하고 비클리포드 처리 오버헤드가 구조적으로 어떻게 나타나는지를 정리했으며[6], Dulek-Schaffner-Speelman은 고전 동형암호를 결합해 다항 크기 회로까지 확장하는 방향을 제시하면서 클리포드는 프레임 갱신으로, 비클리포드는 가젯으로 처리하는 패턴이 양자 동형암호 계열에서 사실상 표준 형태로 자리 잡았다[5].

글로벌 개발 동향에서 두드러지는 점은 양자 동형암호가 이론 연구에만 그치지 않고, 제한적

범위이지만 실험적 구현과 시스템화 시도가 지속적으로 보고되고 있다. 광학 기반에서 양자 완전 동형암호의 실험적 구현을 제시한 연구는 복호화 없는 계산이라는 목표를 장치 수준에서 시연했고[7], 단일 광자 기반 집적 광자 소자에서 동형암호 개념을 적용한 실험도 보고되어 하드웨어 경로로 집적 광자 플랫폼이 유력한 후보로 거론되고 있다[8]. 최근에는 실리콘 포토닉 칩에서 양자 동형암호를 구현하고 클라이언트-서버 구성과 연산 절차를 포함한 실험 결과가 제시되는 등 보안 연산을 네트워크형 구성요소와 함께 묶으려는 방향이 구체화되고 있다[9]. 이러한 실험들은 아직 범용·대규모 회로를 대상으로 하지는 못하지만, 보안 기능이 양자 클라우드에 추가될 때 어떤 형태의 하드웨어 구성과 제어 기능이 필요한지 실증적으로 제시한다는 점에서 중요한 의의가 있다. 암호화된 입력을 서버가 복호화 없이 처리하는 광자 기반 동형암호 실험의 개념적 흐름은 [그림 3]과 같다.



* 클라이언트 암호화-서버 연산-클라이언트 복호·측정 흐름
〈자료〉 Jonas Zeuner et al., "Experimental quantum homomorphic encryption", npj Quantum Information, Vol.7, Article 25, 2021.

[그림 3] 암호화된 입력을 서버가 복호화 없이 처리하는 광자 기반 동형암호 실험 개념도

실용화를 향한 또 다른 흐름은 구현 가능성을 평가하기 위한 소프트웨어 기반 검증과 도구화이다. 비클리포드 처리는 추가 큐비트, 조건부 보정, 키 갱신 절차를 동반하므로 구현 비용이 증가할 수 있으며, 시뮬레이션 연구는 이러한 오버헤드의 병목을 분석하는 데 활용된다. Ganjian 등은 양자 동형암호 구성의 시뮬레이션 구현을 제시하고, 암호화 키 갱신을 포함했을 때의 런타임과 자원 소모를 측정함으로써 비용 병목이 어디에서 발생하는지 정량적으로 보여준다[10]. 이러한 공개 구현과 성능 측정은 클라우드 환경에서 보안 기능을 추가할 때 비클리포드 처리, 키 갱신, 통신 왕복 지연 중 무엇을 우선 최적화해야 하는지 판단하는 기반 자료로 활용될 수 있다.

기밀성 기술 못지않게 클라우드 운영에서는 결과의 무결성과 검증 가능성이 중요해진다. 입력과 결과가 보호되더라도 서버가 연산을 누락하거나 다른 연산을 수행했을 때 이를 탐지할 수 없다면 결과를 신뢰하기 어렵다. 이 문제를 다루기 위해 고전 클라이언트가 양자 서버의 계산을 검증하는 프로토콜이 발전해 왔고, Mahadev는 고전 검증자가 양자 계산 결과를 상호작용적으로 검증할 수 있는 프로토콜을 제시하며 계산적 보안 기반의 검증 가능성을 정리했다[11]. 이후 후속 연구는 효율, 라운드 수, 검증자 부담 등을 개선하는 방향으로 이어지고 있다[12]. 이 계열은 정보 이론적 보안이 아니라 계산적 가정에 기반하지만, 클라우드 서비스 관점에서는 감사 가능성과 품질 보증을 부여하는 현실적 수단이 될 수 있다.

보안 프로토콜이 실제 클라우드에서 작동하기 위해서는 알고리즘 수준의 설계만으로는 충분하지 않고, 런타임과 하드웨어가 제공하는 제어 기능이 필수적으로 따라가야 한다. 특히, 비클리포드 가젯, 오류 보정 절차, 일부 검증 절차는 중간 측정 결과에 따라 후속 연산을 조건부로 수행하며, 이는 중간 측정과 고전 제어 흐름이 가능한 실행 모델을 요구한다. IBM은 Qiskit Runtime 환경에서 고전 피드포워드와 제어 흐름을 지원하는 가이드를 제공하며, 동적 회로 사용 방식과 제약을 명시한다[13]. 또한, 동적 회로 구현을 유틸리티 스케일로 확장해 모든 사용자가 활용할 수 있도록 개선했다고 소개하면서, 동적 회로가 정적 회로로는 접근하기 어려운 프로토콜과 응용을 가능하게 한다는 점을 강조한다[14]. 이러한 흐름은 보안 관점에서도 중요하다. 파울리 프레임 기반 마스킹에서 비클리포드 처리와 키 갱신은 실행 타이밍과 결합하는 경우가 많고, 오류 보정 · 디코딩과도 실행 흐름이 얽히기 때문에, 동적 회로 지원 여부가 보안 기능 탑재 가능성의 전제 조건으로 작동할 수 있다[13][14].

이처럼 글로벌 기술 개발은 파울리 프레임 기반 상태 마스킹을 핵심 기반으로 삼고, 이를

클라우드에서 실제로 구현하기 위한 실험, 시뮬레이션, 검증, 런타임 기능을 동시에 강화하는 방향으로 진행되고 있다. 양자 동형암호 계열에서는 클리포드 구간의 효율성과 비클리포드 처리의 병목이 반복적으로 확인되면서 가젯 및 키 갱신의 최적화가 핵심 과제이다[5][6].

전반적으로 실험적 구현은 아직 제한적이지만 광학 및 집적 광자 플랫폼에서 동형암호 개념을 구현하며 클라이언트-서버 구성의 현실성을 보여주고 있고[7]-[9], 시뮬레이션 기반 도구화는 오버헤드의 성격을 정량적으로 분석하는 방향으로 확장되고 있다[10]. 한편, 결과 검증은 계산적 가정에 기반한 고전 클라이언트 검증으로 발전하며, 신뢰할 수 없는 클라우드 환경에서 무결성을 확보하는 축으로 자리 잡는 중이다[11][12]. 이러한 흐름을 실제 서비스로 묶어내기 위해서는 동적 회로와 같은 런타임 기능이 보편적으로 제공되어야 하며, 측정 · 피드포워드 지연을 낮추는 시스템 최적화가 보안 기능 탑재의 실질적 관문이 될 것으로 보인다[13][14].

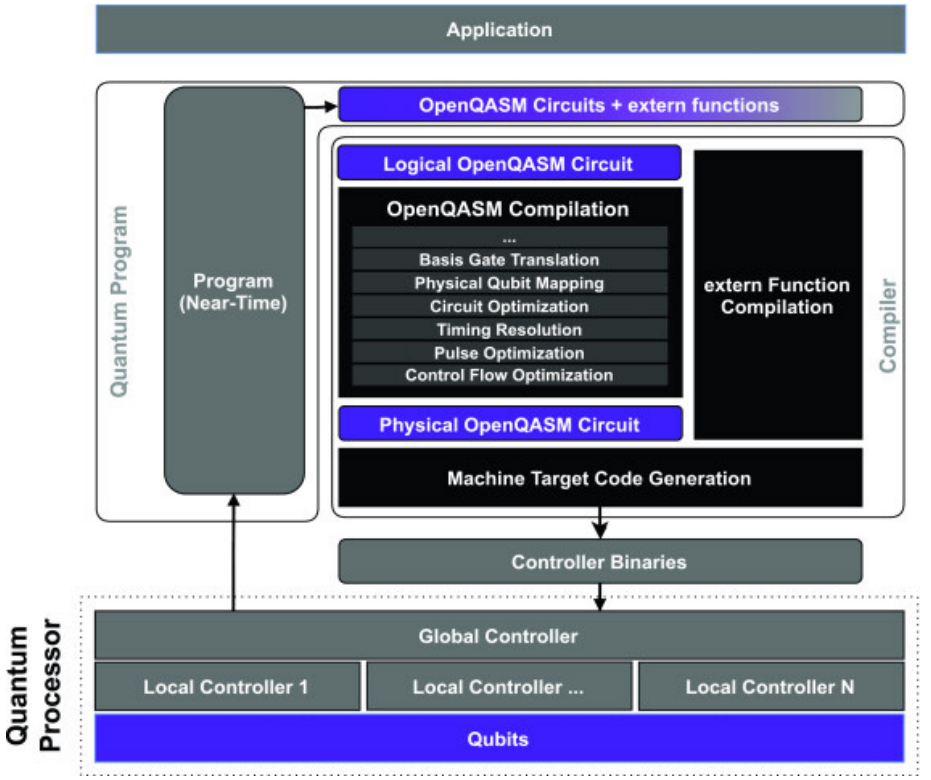
IV. 안전한 양자 클라우드를 위한 표준화 생태계

양자 클라우드에서 신뢰는 단순히 보안 기술을 도입하는 것만으로 확보되지 않는다. 서로 다른 사업자와 소프트웨어 환경에서도 요구사항을 일관되게 해석하고, 실행 결과와 성능을 공통 기준으로 비교할 수 있어야 한다. 이 관점에서 표준화는 생태계의 확장과 조달 · 운영의 제도화 선행 요건이다. 특히, 양자 클라우드는 하드웨어 이질성이 크고 실행 모델이 빠르게 진화하는 영역이어서, 용어 · 정의, 프로그램/회로 기술 방식, 런타임 제어 의미론, 중간 표현과 인터페이스, 성능 지표와 벤치마킹 같은 항목이 정리되지 않으면 서비스 간 상호운용성과 신뢰성 있는 비교가 구조적으로 어렵다[15][16].

표준화의 가장 기초 층은 용어와 정의의 정비이다. ISO/IEC는 양자 기술 전반을 다루기 위해 JTC 3(Quantum technologies)을 운영하며, 양자 정보 기술로서의 양자 컴퓨팅과 시뮬레이션을 포함한 표준화 범위를 명시한다[15]. 용어 차원에서는 ISO/IEC 4879:2024가 양자 컴퓨팅 분야에서 공통적으로 사용하는 용어를 정의하고, 조직 간 개념 교환에 적용될 수 있음을 밝힌다[16]. IEEE에서도 양자 기술 정의를 다루는 P7130 프로젝트가 추진되고 있으며, 호환성과 상호운용성을 위해 용어 명확화가 필요하다는 취지를 제시한다. 이 층의 표준이 갖는 실무적 의미는 같은 단어가 다른 의미로 쓰이는 상황을 줄이는 데 있다. 양자

클라우드 보안 논의에서도 '프레임', '제어 흐름', '동적 회로', '벤치마크' 같은 핵심 용어가 공급자 문서와 연구 문헌에서 미묘하게 다르게 사용되기 쉬운데, 용어 표준이 정립될수록 정책 문서, 조달 요구조건, 서비스 수준 협약(Service Level Agreement: SLA)에서의 모호성이 줄어든다[16].

용어 다음으로 중요한 층은 실행 모델을 기술하는 언어와 의미론의 정비이다. 보안 기능이 포함된 양자 클라우드에서 실제로 문제가 되는 것은 "회로를 보낸다"는 표현이 더 이상 단순한 게이트열을 의미하지 않는다는 점이다. 중간 측정 결과에 따른 조건부 분기, 실행 중 고전 계산, 시간·타이밍 제약 같은 요소가 포함되면서 회로 기술 언어가 사실상 런타임 표준의 역할을 수행하게 된다[17][18]. OpenQASM 3.0은 측정 기반 회로 모델을 전제로 하면서 측정 결과에 따른 고전 피드포워드 제어 흐름을 지원하는 언어로 소개되고[17], OpenQASM



〈자료〉 A. W. Cross et al., "OpenQASM 3: A Broader and Deeper Quantum Assembly Language", ACM Transactions on Quantum Computing, 2022.

[그림 4] 양자 프로그램의 컴파일·실행 흐름에서 OpenQASM의 위치와 역할

3의 확장 목적이 단순 회로 표기뿐만 아니라 양자-고전 상호작용이 있는 실시간 도메인까지 포괄하는 것으로 제시된다[18]. 이는 보안 프로토콜의 관점에서도 직결된다. 보안 연산은 흔히 실행 중 조건부 보정, 측정 기반 분기, 런타임 고전 계산을 수반할 수 있는데, 이러한 기능이 언어 차원에서 표준화되어야 공급자별로 다른 임시 API에 종속되지 않고 재현이 가능한 방식으로 구현·검증될 수 있다[17][18]. 양자 프로그램의 컴파일·실행 흐름에서 OpenQASM이 차지하는 위치와 역할은 [그림 4]와 같다.

언어 계층과 함께 상호운용성을 좌우하는 것은 중간 표현(Intermediate Representation: IR)과 인터페이스의 표준화이다. 중간 표현은 서로 다른 언어로 작성된 프로그램을 실제 실행 환경이 이해할 수 있는 공통 형식으로 바꾸는 중간 단계의 표현을 뜻한다. 이러한 환경에서 회로·프로그램을 어떤 공통 형식으로 주고받는가는 생태계의 결합 비용을 결정한다[19][20]. 양자 중간 표현(Quantum Intermediate Representation: QIR)은 LLVM(Low Level Virtual Machine) 프로젝트의 범용 중간 코드 표현인 LLVM IR 위에서 양자 프로그램을 표현하기 위한 규칙이며, QIR Alliance의 qir-spec 문서는 이를 명시적으로 설명한다[19].

Microsoft 문서 역시 QIR을 언어·프레임워크와 대상 플랫폼 사이의 공통 인터페이스로 소개하며, 하드웨어와 언어에 종속되지 않는 형식으로 양자 프로그램을 표현한다[20]. 보안 관점에서 IR 표준화가 중요한 이유는 보안 기능이 컴파일 단계 전처리 또는 런타임 계측으로 삽입되는 경우가 많기 때문이다. 특정 공급자 SDK에만 존재하는 메타데이터나 프라그마에 의존하면 동일한 보안 동작을 다른 환경에서 재현하기 어렵고, 검증이나 감사도 공급자 종속으로 남는다. 반대로 IR이 공통화되면, 보안 관련 변환과 계측을 IR 레벨에서 일관되게 정의하고, 타깃별 구현 세부는 백엔드가 흡수하는 구조로 발전시킬 수 있다[19][20].

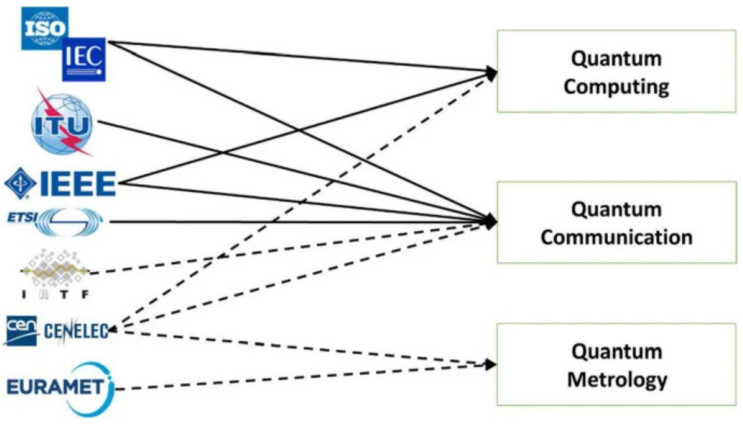
신뢰 기반 생태계에서 빠질 수 없는 표준화 축은 성능 지표와 벤치마킹이다. 보안 기능은 대체로 오버헤드를 동반하며, 그 오버헤드는 단순히 회로 깊이 증가로만 나타나지 않고 중간 측정 지연, 조건 분기 처리 능력, 런타임 고전 계산 지연, 통신 왕복 지연 같은 시스템 지표로 나타난다. 따라서 보안 기능을 켰을 때 어떤 비용이 추가되는가를 비교가 가능한 형태로 측정할 수 있어야 서비스 선택과 조달이 가능해진다. IEEE P7131은 양자 컴퓨팅 하드웨어·소프트웨어의 성능 지표와 벤치마킹 표준화를 목표로 하는 워킹그룹으로 소개된다. 이러한 벤치마킹 표준의 중요성은 보안 관점에서 더 커진다. 예를 들어, 동적 제어를 요구하는 보안 기능은 정적 회로 처리량이 아니라 제어 흐름을 포함한 실행 능력에 의해 성패가 갈릴 수

있으므로, 장기적으로는 벤치마크 항목이 정적 게이트 성능에 머물지 않고 실행 모델 특성까지 포괄하도록 진화할 필요가 있다[17]. 이는 표준화가 단지 측정 항목을 나열하는 작업이 아니라, 무엇을 서비스 품질로 볼 것인지에 대한 합의를 형성하는 과정이다.

표준화 논의는 컴퓨팅에 국한되지 않고 배치와 운영의 프레임으로 확장되는 흐름도 나타난다. ETSI는 TC Quantum Technologies(TC QT)를 통해 양자 기술과 그 배치에 대한 기술 보고서(TR) 및 규범적 기술 규격(TS) 개발을 촉진한다고 밝히고 있으며, 적용 영역으로 보안 통신, 고도 네트워킹, 센싱 등을 언급한다[21]. 양자 클라우드 보안은 통신 표준과 직접 동일하지는 않지만, 실제 배치와 운영의 관점에서 상호운용 가능한 구성요소와 운영 상의 보안 요구사항을 체계화한다는 점에서 같은 논리를 따른다[21]. 향후 양자 클라우드가 데이터센터 인프라, 네트워크, 접근제어, 감사 체계와 결합되면, 양자 실행 기능 자체뿐 아니라 운영·관리 인터페이스의 표준화도 사실상 신뢰 생태계의 일부가 된다[21].

종합하면, 신뢰 기반 양자 클라우드 생태계에서 표준화는 용어를 통일하는 단계에 머물지 않고, 실행 모델을 기술하는 언어, 컴파일·실행을 연결하는 IR과 인터페이스, 서비스 품질을 비교하는 벤치마킹 지표, 그리고 배치·운영 관점의 요구사항으로 확장되는 방향으로 전개되고 있다[15]-[17][19]-[21]. 이러한 주요 표준화 기구별·양자 기술 분야별 표준화 활동의 분포는 [그림 5]와 같다.

현재의 표준화 흐름은 보안 기법 자체의 수학적 내용을 직접 표준으로 고정하기보다, 이를



〈자료〉 van Deventer et al., “Towards European standards for quantum technologies”, EPJ Quantum Technology, 2022.

[그림 5] 주요 표준화 기구와 양자 기술 분야 간 표준화 활동 분포

서비스 환경에서 구현 · 연동하기 위한 공통 언어와 상호운용 구조를 먼저 마련하는 데 초점을 두고 있다[15][16]. 이와 같은 접근은 기술 변화 속도가 빠른 영역에서 혁신을 저해하지 않으면서도, 산업 생태계를 확장할 수 있게 더욱 실용적인 방향이다[15][21].

V. 결론

양자 컴퓨팅은 장비 구축과 운영 비용, 하드웨어 제약으로 인해 단기간에는 클라우드 기반 위임 사용 모델이 주류가 될 가능성이 크다. 이 환경에서 사용자는 통신 구간 보호만으로는 부족하며, 연산이 수행되는 동안의 데이터 기밀성과 결과 신뢰성을 요구하게 된다. 본 고는 이러한 요구를 중심으로 파울리 프레임 기반 상태 마스킹, 암호화된 상태 위 연산의 실용 조건 그리고 표준화 · 상호운용성 흐름을 정리하였다.

기밀성 측면에서 파울리 프레임 기반 마스킹은 위임 환경에서 “데이터 자체”를 직접 보호하는 가장 기본적이고 강력한 기반 중 하나이다.

그러나 실서비스 관점에서 핵심은 마스킹 자체보다 연산 과정에서 키가 어떻게 변하는지를 정확히 추적하고 반영하는 운용 능력이다. 클리포드 구간은 프레임 갱신만으로 처리 가능하지만, 비클리포드 구간에서는 보정과 추가 자원이 필요해 비용이 증가하며, 이 오버헤드가 현재 하드웨어에서 실용화를 제한하는 주요 요인으로 작용한다.

신뢰성 측면에서는 기밀성만으로 충분하지 않다. 서버가 연산을 누락하거나 다른 연산을 수행했을 때 이를 탐지할 수 없다면 결과를 신뢰하기 어렵다. 따라서 무결성과 검증 가능성은 보안 기능을 감사 가능성과 품질 보증으로 확장하는 필수 요소이며, 실제 적용 여부는 동적 제어, 조건부 분기, 피드포워드 같은 런타임 기능 제공 수준에 좌우된다.

이는 표준화 · 상호운용성과 직접 연결된다. 용어와 정의가 정리되지 않으면 요구사항이 사업자별로 다르게 해석되고, 회로와 실행 제어를 표현하는 방식이 통일되지 않으면 구현이 공급자 종속으로 고착되며, 성능 지표와 벤치마킹이 정립되지 않으면 보안 기능의 비용과 효과를 비교할 수 없다. 결국, 안전한 양자 클라우드의 실용화는 개별 보안 기법 채택을 넘어, 기밀성과 검증을 런타임 능력으로 구현하고 이를 표준화된 방식으로 표현 · 연동 · 비교할 수 있게 만드는 생태계 과제이다. 먼저, 보안 오버헤드의 측정 체계와 동적 실행 기능의 제공 범위를 명확히 해야 한다. 이어서 중기적으로는 언어 · IR · API 상호운용성을 강화해 공급자

종속을 줄이며, 장기적으로는 결함 허용 운영과 결합한 프레임 기반 보안 연산이 클라우드의 기본 요건으로 흡수되는 방향으로 발전할 필요가 있다.

참고문헌

[1] J. Preskill, "Quantum Computing in the NISQ era and beyond", Quantum, Vol.2, 2018. 8. 6, p.79(doi:10.22331/q).

[2] A. Broadbent, J. Fitzsimons and E. Kashefi, "Universal Blind Quantum Computation", Proc. 50th IEEE FOCS, 2009, pp.517-526.

[3] J. F. Fitzsimons, "Private quantum computation: an introduction to blind quantum computing and related protocols", npj Quantum Information, Vol.3, Article 23, 2017(doi:10.1038/s41534-017-0025-3).

[4] K. A. G. Fisher et al., "Quantum computing on encrypted data", Nature Communications, Vol.5, Article 3074, 2014(doi:10.1038/ncomms4074).

[5] Y. Dulek, C. Schaffner and F. Speelman, "Quantum homomorphic encryption for polynomial-sized circuits", Cryptology ePrint Archive, Paper 2016/559, 2016(CRYPTO 2016).

[6] A. Broadbent and S. Jeffery, "Quantum homomorphic encryption for circuits of low T-gate complexity", Cryptology ePrint Archive, Paper 2015/551, 2015(CRYPTO 2015).

[7] W. K. Tham et al., "Experimental Demonstration of Quantum Fully Homomorphic Encryption with Application in a Two-Party Secure Protocol", Phys. Rev. X, Vol.10, Article 011038, 2020 (doi:10.1103/PhysRevX.10.011038).

[8] J. Zeuner et al., "Experimental quantum homomorphic encryption", npj Quantum Information, Vol.7, Article 25, 2021(doi:10.1038/s41534-020-00340-8).

[9] Y. Li et al., "Experimental Quantum Homomorphic Encryption Using a Quantum Photonic Chip", Phys. Rev. Lett., Vol.132, Article 200801, 2024(doi:10.1103/PhysRevLett.132.200801).

[10] S. Ganjian, C. Paddock and A. Broadbent, "Demonstrating Quantum Homomorphic Encryption Through Simulation", Proc. 2024 IEEE Int. Conf. Quantum Computing and Engineering(QCE), 2024 (doi:10.1109/QCE60285.2024.10421).

[11] U. Mahadev, "Classical Verification of Quantum Computations", Proc. 59th IEEE FOCS, 2018 (doi:10.1109/FOCS.2018.00033; arXiv:1804.01082).

[12] N.-H. Chia, K.-M. Chung and T. Yamakawa, "Classical Verification of Quantum Computations with Efficient Verifier", Cryptology ePrint Archive, Paper 2020/1273, 2020(TCC 2020).

[13] IBM Quantum Documentation, "Classical feedforward and control flow(dynamic circuits)", https://docs.quantum.ibm.com/guides/classical-feedforward-and-control-flow

[14] J. Yu et al., "Utility-scale dynamic circuits now available for all users", IBM Quantum Blog, 19 Nov. 2025.

[15] IEC/ISO JTC 3, “Quantum technologies(committee scope)”, ISO, https://www.iso.org/committee/10138914.html
[16] ISO/IEC, “ISO/IEC 4879:2024 Information technology — Quantum computing — Vocabulary”, ISO, https://www.iso.org/standard/80432.html
[17] OpenQASM, “OpenQASM 3.0 Specification”, https://openqasm.com/versions/3.0/
[18] A. W. Cross et al., “OpenQASM 3: A broader and deeper quantum assembly language”, ACM Transactions on Quantum Computing, Vol.3, No.3, Article 12, 2022(doi:10.1145/3505636).
[19] QIR Alliance, “QIR Specification(qir-spec)”, GitHub, https://github.com/qir-alliance/qir-spec
[20] Microsoft, “Quantum Intermediate Representation(QIR)”, Microsoft Learn, https://learn.microsoft.com/en-us/azure/quantum/concepts-qir
[21] ETSI, “Quantum Technologies(QT)”, https://www.etsi.org/technical-groups/qt/
[22] O. van Deventer et al., “Towards European standards for quantum technologies”, EPJ Quantum Technology, Vol.9, Article 33, 2022(doi:10.1140/epjqt/s40507-022-00150-1).