프라이버시 보호 양자 컴퓨팅 연구 동향

Trends in Privacy-Preserving Quantum Computing Research

이영경 (Y.K. Lee, youngklee@etri.re.kr) 암호공학연구실 선임연구원

ABSTRACT

Quantum computers can likely perform computations that are unattainable by classical computers, and they represent the next generation of computing technologies. Due to high costs and complex maintenance, direct ownership of quantum computers by individuals users is challenging. Future utilization is predicted to involve quantum computing servers performing delegated computations for clients lacking quantum capabilities, similar to the current utilization of supercomputing. This delegation model allows several users to benefit from quantum computing without requiring ownership, thereby providing innovation potential in various fields. Ensuring data privacy and computational integrity in this model is critical for ensuring the reliability of quantum cloud computing services. However, these requirements are difficult to achieve because classical security techniques cannot be directly applied to quantum computing. We review research on security protocols for the delegation of quantum computing with focus on data privacy and integrity verification. Our analysis covers the background of quantum computing, privacy-preserving quantum computational models, and recent research trends. Finally, we discuss challenges and future directions for secure quantum delegated computations, highlighting their importance for the commercialization and widespread adoption of quantum computing.

KEYWORDS MBQC, UBQC, 암호프로토콜, 양자계산, 양자동형암호, 양자 서버, 양자위임계산

Ⅰ. 서론

양자 컴퓨터는 기존의 고전 컴퓨터로는 불가능한 계산을 수행할 수 있는 잠재력을 지닌 차세대 컴퓨팅 기술이다. 양자 컴퓨터는 높은 비용과 복잡한 유지 보수 문제로 인해 일반 사용자들이 직접 소유하기 어렵다. 근 미래에는 현재의 슈퍼컴퓨터 활용 형태와 비슷하게 양자 컴퓨팅 서버가 양자 계산 능력이 없거나 부족한 클라이언트의 양자 계산을 위임받아 수행하는 것이 주요 활용 모델이 될 것으로 예측된다. 이러한 양자 서버 위임 계산 모델은 양자 컴퓨터를 직접 소유하지 않고도 다수의 이용자가 그

* DOI: https://doi.org/10.22648/ETRI.2024.J.390505
* This work was supported by Electronics and Telecommunications Research Institute(ETRI) grant funded by the Korean government[24ZS1320, Research on Quantum-Based New Cryptographic System for Ensuring Perfect Data Privacy].

본 저작물은 공공누리 제4유형
출처표시+상업적이용금지+변경금지 조건에 따라 이용할 수 있습니다.
©2024 한국전자통신연구원

이점을 누릴 수 있게 하며, 연구자와 기업 등 양자 계산을 해야 하는 다양한 분야에 혁신적인 활용 가능성을 제공할 수 있을 것이다.

양자 계산 위임 모델이 상용화되기 위해서는 클라이언트의 민감한 정보를 양자 서버에 노출하지 않고, 양자 서버가 계산을 정직하게 수행했는지 확인할 수 있는 보안 프로토콜이 필요하다. 하지만, 양자 위임 계산 모델에서 양자 서버와 클래식 클라이언트 간의 데이터 보안 및 계산 무결성을 보장하기는 쉽지 않다. 기존의 데이터 보안 기술과 무결성 검증 기술은 클래식 컴퓨팅을 기반으로 설계되어 양자 서버의 양자 계산에 직접 적용될 수 없기 때문이다.

본고에서는 이러한 문제를 해결하기 위한 양자 위임 계산 모델에서 데이터 보안과 무결성 검증 등의 보안 기술 연구 현황을 살펴보고자 한다. Ⅱ장에서는 양자 정보 이론 관점에서 양자 컴퓨팅 배경지식을 다루고, Ⅲ장에서는 프라이버시 보호 양자 컴퓨팅 모델, Ⅳ장에서는 최신 연구 동향을 다루고, Ⅴ장에서 결론을 맺는다.

Ⅱ. 양자 컴퓨팅 계산 모델

본 장에서는 본고에서 다룰 프라이버시 보호 양자 컴퓨팅 연구 동향 이해에 필요한 기본지식을 다룬다. 양자 정보이론 관점에서의 양자 컴퓨터 배경지식과 양자 컴퓨팅 계산 모델인 회로 기반 계산과 양자 컴퓨팅의 특성을 활용한 계산 모델인 측정 기반 계산 모델에 대해 살펴본다.

1. 기본구성

가. 큐빗 & 블로흐 구면(Bloch sphere)

고전 컴퓨팅 모델에서 0 또는 1의 값을 가지는 비트는 가장 기본적인 구성요소이다. 양자 컴퓨팅에서는 비트에 대비되는 양자 비트(큐빗)를 이용한다. 큐빗은 이차원의 복소수 공간에서 정의되는데 기본적으로 $|0\rangle$상태와 $|1\rangle$상태의 베이시스(Basis)를 이용하여 스칼라값이 복소수인 벡터 $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$로 표현할 수 있다. 이때, $||\alpha||^2$, $||\beta||^2$는 각각 기본 베이시스($\{|0\rangle, |1\rangle\}$)로 측정할 때 해당 값으로 관측될 확률을 나타낸다. 양자 컴퓨터에서 중첩을 간단히 보여주는, $|\pm\rangle = 1/\sqrt{2}(|0\rangle \pm |1\rangle)$ 상태는 기본 베이시스로 관측할 때 1/2의 확률로 $|0\rangle$또는 $|1\rangle$로 관측된다. 즉, $|0\rangle$상태와 $|1\rangle$상태의 중첩을 의미하는 상태인 것이다.

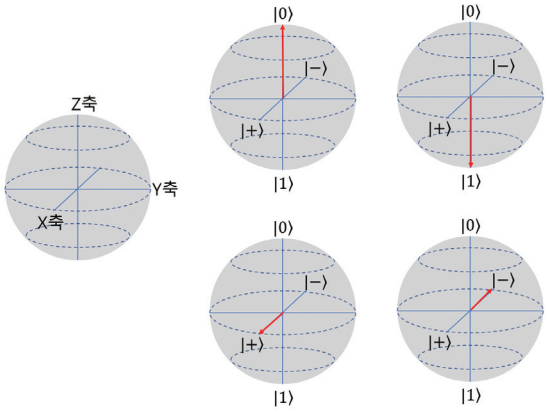

그림 1 블로흐 구면과 양자 상태

블로흐 구면은 그림 1과 같이 단일 큐빗을 3차원(복소평면[2차원]과 실수[1차원]) 공간에 나타낸 것으로 시각적인 설명을 통해 큐빗의 상태와 변화를 설명하는 좋은 도구로 활용된다.

나. 양자 게이트

양자 컴퓨팅에는 단일 혹은 다중 큐빗의 상태 변환을 수행하는 다양한 게이트가 있다. 기본적인 X, Y, Z 게이트는 블로흐 구면으로 보면 각 축을 중심으로 180도 회전시키는 단일 큐빗 게이트이다. 예를 들어 $|0\rangle$상태에 X 게이트를 적용하면 X축으로 180도 회전하여 $|1\rangle$상태로 바뀌게 되고, $|+\rangle$상태에 Z

게이트를 적용하면 Z축으로 180도 회전하여 $|-\rangle$ 상태로 바뀌게 된다(그림 1 참고).

임의의 양자 계산을 수행하기 위해서는 범용(Universal) 게이트 집합이 필요하다. *H*: 하다마드 게이트, *CZ*: 컨트롤드*Z* 게이트, *R(θ)*: 로테이션 게이트는 범용 게이트 집합 구성에서 중요한 게이트이다. *H* 게이트는 $|0\rangle$을 $|+\rangle$로, $|1\rangle$을 $|-\rangle$로 바꿔주며, 블로흐 구면으로 보면 *XZ*평면에서 *X*축에서 45도 기울어진 축으로 180도 회전시킨다. *CZ* 게이트는 두 개의 큐빗에 동작하는 게이트로 하나의 큐빗 상태가 $|1\rangle$일 때, 나머지 큐빗에 *Z* 게이트가 적용되는 게이트이다. *R(θ)* 게이트는 *Z*축을 중심으로 θ 각 만큼 회전시키는 게이트이다.

다. 측정

양자 컴퓨팅에서 양자 상태를 측정한다는 것은 보통 임의의 양자 상태 $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$를 기본 베이시스($|0\rangle$과 $|1\rangle$)로 관측하여 확률에 따라 $|0\rangle$ 혹은 $|1\rangle$로 양자 상태가 붕괴되는 과정을 의미한다. $|0\rangle$인 양자 상태를 관측한다면 100%의 확률로 $|0\rangle$으로 관측될 것이고, 양자 상태를 관측하면 $|0\rangle$또는 $|1\rangle$이 각각 50%$|\pm\rangle = 1/\sqrt{2}(|0\rangle \pm |1\rangle)$ 확률로 관측된다.

하지만 $|+\rangle$상태를 기본 베이시스가 아닌 $\{|+\rangle, |-\rangle\}$ 베이시스로 관측하면 100% 확률로 $|+\rangle$로 결정된다. 뒤에서 설명할 측정 기반 계산 방식에서는 기본 베이시스로 관측하는 것 외에도 다음과 같은 베이시스를 사용한다.

$$|\pm_\theta\rangle = 1/\sqrt{2}(|0\rangle \pm e^{i\theta}|1\rangle).$$

이 베이시스는 θ이 0일 때, $\{+\rangle, -\rangle\}$ 베이시스가 된다. 기본 베이시스가 *Z*축 ($\{|0\rangle, |1\rangle\}$)으로 관측하는 것이라면 *X*축으로 관측하는 것은 ($\{|+\rangle, |-\rangle\}$) 베이시스로 관측하는 것과 같다. θ가 0이 아닌 경우에는 *XY*평면에 놓인 *X*축이 θ만큼 회전된 축으로 관측하는 것으로 볼 수 있다.

2. 회로 기반 계산

회로 기반(Circuit-based) 양자 계산은 양자역학의 원리를 이용한 양자 컴퓨팅에 흔히 사용되는 계산 모델로, 고전적 컴퓨팅의 회로와 유사하다. 이 모델에서는 0 또는 1의 값을 나타내는 고전비트와 달리 여러 상태를 동시에 가질 수 있는 양자 중첩 능력을 가지는 큐빗을 입력과 출력으로 사용한다. 양자 게이트는 큐빗에 유니터리 변환을 적용해 양자 연산을 수행하며, 하다마드 게이트, *CNOT* 게이트, 페이즈 게이트 등이 사용된다. 이러한 게이트들은 양자 회로 내에서 특정 순서로 배열되어 양자 알고리즘을 실행한다. 양자 얽힘은 큐빗들 사이의 복잡한 상관관계를 형성하여 양자 계산에 필수적으로 사용된다. 계산의 최종 결과는 큐빗의 측정을 통해 얻어지며, 이 과정은 큐빗의 상태를 기저 상태로 붕괴시키게 된다.

3. 측정 기반 계산

측정 기반 양자 계산(MBQC: Measurement-Based Quantum Computation)은 전통적인 회로 모델이 아닌 다양한 베이시스를 사용한 측정을 통해 양자 계산을 수행하는 방식이다. MBQC에서는 대규모의 고도로 얽힌 양자 상태인 자원 상태를 사용하며, 흔히 클러스터 상태를 사용한다. 클러스터 상태는 그림 2와 같이 각 큐빗이 인접한 큐빗과 얽혀 있는 격자 구조로 이루어져 있다. 양자 계산은 자원 상태의 개별 큐빗에 대한 측정을 통해 진행되는데, 이 측정에 사용될 측정 베이시스와 순서가 구현할 양자 알고리즘을 결정하게 된다. 이때, 개별 큐빗의 측정 결과는 다음 측정의 베이시스를 결정하는 데 사용되므로,

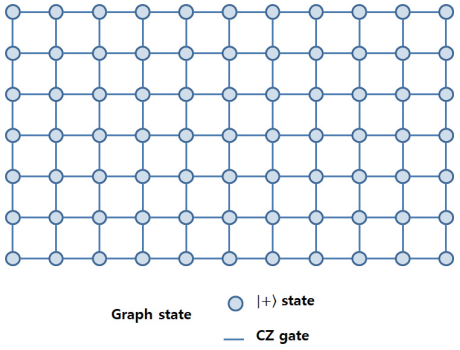

그림 2 클러스터 양자 상태

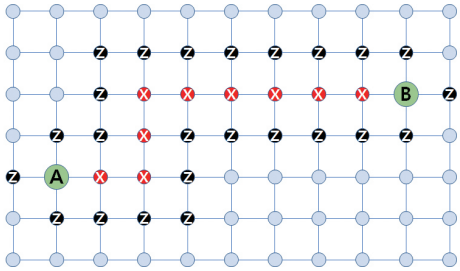

그림 3 MBQC기반의 Bell 양자 상태

측정은 적응적으로(Adaptive) 이루어져야 한다. 또한, 해당 과정에서 양자 정보의 손실을 보정하고 오류를 수정하는 메커니즘이 필요하다.

MBQC는 모든 큐빗의 측정이 완료되면 양자 알고리즘을 적용한 클러스터 상태를 재사용할 수 없으므로 일방향(One-way) 양자 컴퓨팅이라고도 한다. MBQC는 양자 계산을 이해하고 사용하는 새로운 접근 방식을 제공하기도 한다. 전통적인 회로 기반의 양자 컴퓨팅이 아닌 점에서 비롯되는 특징을 이용하여 암호학, 최적화, 시뮬레이션 등 다양한 분야에서 MBQC를 응용하고 있다.

가. MBQC 양자 상태 준비

MBQC에서 첫 번째 과정인 그래프 양자 상태 준비과정은 다음과 같다. 먼저 노드와 엣지로 구성되는 그래프 형태를 구성하는데 노드는 하나의 물리적 큐빗으로 $|+\rangle$상태에 대응되고 엣지 두 노드에 적용하는 CZ 게이트에 대응된다. 이차원에서의 클러스터 양자 상태는 레티스 형태로, 모든 노드가 $|+\rangle$상태이며 상하좌우 노드들과 CZ 게이트를 적용하여 구성한다(그림 2 참고).

그림 3과 같이 클러스터 양자 상태에서 Z축, X축 관측 등 다양한 베이시스를 활용하여 관측만으로 Bell 양자 상태를 만들어 낼 수 있다.

나. MBQC 측정을 통한 계산

MBQC에서 두 번째 과정인 측정을 통한 계산은 양자 게이트 텔레포테이션 원리가 이용된다. 입력 큐빗인 임의의 양자 $|\Psi\rangle$(첫 번째 큐빗) 상태와 준비된 $|+\rangle$상태(두 번째 큐빗)가 CZ 게이트로 얽혀 있는 상태에서 첫 번째 큐빗을 $|\pm_\theta\rangle = 1/\sqrt{2}\,(|0\rangle \pm e^{i\theta}|1\rangle)$ 베이시스로 관측하게 되면 두 번째 큐빗은 관측 결과에 따라 $HR(\theta)\ |\Psi\rangle$(첫 번째 큐빗: $|+_\theta\rangle$ 또는 $XHR(\theta)\ |\Psi\rangle$(첫 번째 큐빗: $|-_\theta\rangle$)상태로 바뀌게 된다. 즉 첫 번째 큐빗을 관측하는 베이시스에 따라 두 번째 큐빗 상태가 H 게이트와 $R(\theta)$ 게이트가 적용된 입력 큐빗 상태로 변하는 것이다. 이러한 양자 상태 및 게이트 텔레포테이션 원리를 활용하여 관측만을

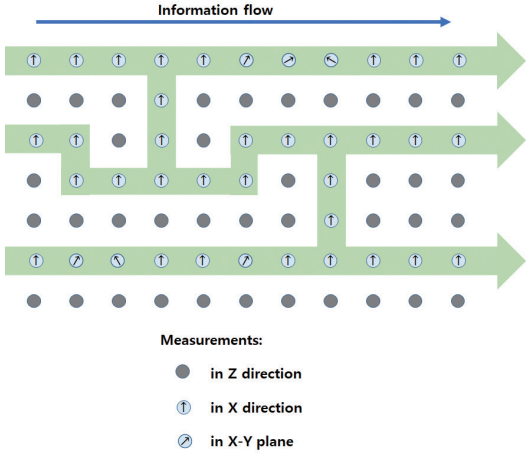

그림 4 MBQC 계산 과정

통해 입력 상태 큐빗에 여러 게이트를 적용하여 회로 기반 양자 컴퓨팅과 같은 계산을 수행할 수 있는 것이다(그림 4 참고). 관측 결과에 따라 의도치 않은 X 게이트가 다음 큐빗에 적용되기 때문에 이를 정정하기 위한 관측 베이시스 조정이 필요하다.

Ⅲ. 프라이버시 보호 양자 컴퓨팅

근 미래에 양자 컴퓨터가 활용되는 모습은 현재 슈퍼컴퓨터를 활용하는 형태와 비슷할 것으로 보인다. 그림 5와 같이 양자 계산 리소스가 풍부한 양자 서버와 양자 계산 리소스가 없거나 적은 클라이언트가 서버에 양자 계산을 위임하는 형태가 주요할 것으로 예상된다. 양자 컴퓨터를 클라우드 컴퓨팅 서버로 활용하는 것은 다양한 장점이 있다. 양자 컴퓨터는 고가의 장비로 일반 사용자가 소유하기 어려우며 설치 및 유지 보수 비용이 많이 들기 때문에 서버로 이용하면 접근성 및 비용 효율성을 높일 수 있다. 또한, 양자 컴퓨터를 소유할 수 없는 사용자의 현실적 제약을 극복하여, 연구자와 기업이 이를 활용한 연구와 혁신적 기술 개발에 큰 도움을 줄 수 있다. 일반 사용자들을 양자 컴퓨팅 및 알고리즘과 관련된 연구와 기술 개발에 참여시켜 양자 컴퓨터의 발전을 가속화할 수 있다.

그러나 양자 컴퓨터를 서버로 활용하여 위임 계산을 해주는 양자 클라우드 컴퓨팅 모델은 해결해야 할 다양한 보안 문제점을 가진다. 먼저 양자 고전

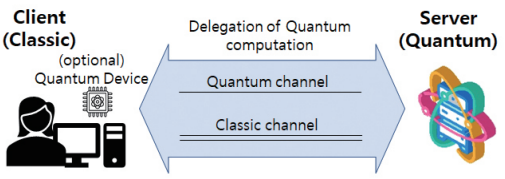

그림 5 양자 서버와 고전 클라이언트 간 계산 위임 모델

컴퓨팅을 사용하는 클라이언트가 요청하고자 하는 양자 계산에 대한 정보를 양자 서버에 전달해야 하는데 민감한 정보를 포함하고 있다면 이를 양자 서버에 노출할 수 있다. 고전적인 서버-클라이언트 간 정보 노출 없이 계산을 위임하는 암호학적 프로토콜 또는 이를 가능하게 하는 동형 암호 등은 연구가 많이 되어왔다. 하지만 양자 서버와 고전 클라이언트 간의 모델에서는 해당 방식이 적용될 수 없거나 동형 암호로 암호화된 데이터를 이용한 양자 위임 계산은 매우 비효율적이다. 또한, 양자 서버가 고전 클라이언트의 요청대로 양자 계산을 정직하게 수행했는지 확인할 수 있는 검증 방식도 필요하다.

정보를 숨기면서 양자 서버에 고전 클라이언트가 양자 계산을 위임하는 모델에서 양자 서버는 양자 컴퓨팅 리소스를 많이 가지고 있지만, 클라이언트는 제한적인 양자 리소스만 사용하거나 양자 컴퓨팅 리소스가 없다. 양자 비밀 계산은 현재 이론적인 연구가 활발히 진행되고 있으며, 기술 적용 시 클라이언트 측에서 필요한 양자 컴퓨팅 리소스를 줄여나가는 방향으로 연구가 진행되고 있다. 양자 서버에 프라이버시 보호 기술이 적용된 계산 검증 가능한 양자 위임 계산 기술이 개발된다면 양자 서버-고전클라이언트 간 양자 위임 계산 서비스가 활발히 활용될 수 있을 것으로 기대된다.

Ⅳ. 양자 비밀 계산 연구 동향

본 장에서는 양자 서버와 고전 클라이언트 간 계산 위임 모델에서 양자 비밀 계산에 관련된 연구 동향을 살펴본다. 먼저 기본적인 양자 계산 모델인 회로 기반의 양자 계산 모델에서의 양자 비밀 프로토콜 및 암호화된 양자 상태 계산 분야의 연구 동향을 살펴보고, 다음으로는 측정 기반 양자 계산 모델에 특화된 양자 비밀 계산 프로토콜 분야의 연구 동향

을 살펴본다.

1. 회로 기반 양자 비밀 계산

가. 데이터 프라이버시 보호 양자 계산

2001년 Childs는 양자 컴퓨팅 서버와 양자 상태 생성/전송 및 X, Z 게이트, 양자 상태 관측 등의 기본적인 양자 컴퓨팅 리소스를 가지는 클라이언트 간의 정보 노출을 하지 않는 양자 위임 계산 프로토콜을 제시하였다[1]. 해당 프로토콜은 암호학적으로 가장 강한 안전성에 해당하는 확률론적 안전성(Probabilistic Security)을 제공하는 OTP(One-Time Pad) 기술을 활용한다. 고전 컴퓨팅에서 OTP는 암호화하고자 하는 평문 비트열의 길이만큼의 키가 필요하며 키와 평문을 XOR 연산하여 암호화한다. Childs의 프로토콜은 양자 상태 버전의 OTP[2]를 활용한다. 그림 6과 같이 양자 OTP에서 키는 한 개의 큐빗당 2비트가 필요하며, 암호화 방법은 키의 첫 번째 비트가 1이면 X 게이트를, 두 번째 비트가 1이면 Z 게이트를 각각 적용하는 것이다.

비밀 계산 프로토콜은 양자 OTP를 이용하여 암호화된 양자 상태를 양자 서버에 전송하여 필요한 게이트 연산을 요청하는 것으로 시작한다. 서버가 수행한 게이트 연산이 적용된 양자 상태를 다시 받은 클라이언트는 OTP 키를 이용하여 복호화하여 위임 연산 결과를 얻는다. 요청하는 게이트 연산에 따라 기존 양자 상태의 암호화 방식이 변형되기 때문에 적용된 게이트에 맞는 복호화 방식을 적용하여 요청 연산 결과가 적용된 평문으로 복호화할 수 있다. 예를 들어, 임의의 양자 상태를 OTP 키와 X, Z 게이트 순으로 암호화한 양자 상태를 서버에 전송하고, 서버는 H 게이트를 위임 연산을 수행하고 클라이언트에게 전송한다고 하자. 이때, 클라이언트를 평문 양자 상태에 H 게이트가 적용된 양자 상태를 얻기 위해서는 Z, X 게이트 순으로 복호화를 진행해야 한다.

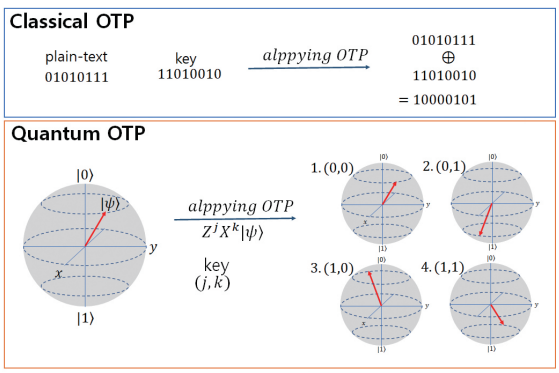

그림 6 양자 One-Time Pad

Childs는 H, $CNOT$, T 집합에 대해 비밀 계산을 수행할 수 있는 프로토콜을 제시하였다. 양자 OTP로 암호화하게 되면 서버가 클라이언트의 양자 상태를 관측하여 정보를 빼내고자 하는 공격도 확률론적 안전성을 바탕으로 방어할 수 있다. 해당 연구는 이론적으로 정보 노출 없이 양자 컴퓨팅 리소스가 부족한 클라이언트가 양자 서버에 게이트 연산을 위임하는 방법을 처음으로 제시하였다.

나. 암호화된 양자 상태 계산

2014년 Fisher 등은 Childs의 회로 기반 양자 비밀 계산 프로토콜 연구를 확장하여 암호화된 양자 상태 데이터를 입력으로 양자 계산하는 프로토콜을 제시하였다[3]. Childs의 기법의 특징은 적용하는 게이트마다 양자 OTP에 사용된 X, Z 게이트 적용 여부에 따른 복호화 방식이 달라진다. 이로 인해 연속적인 위임 게이트 연산이 어렵다. 위임 게이트 연산 후 다른 위임 게이트 연산을 수행하기 위해서는 매번 클라이언트가 첫 번째 위임 게이트 연산 후 변형된 방식으로 복호화하고 새롭게 양자 OTP 암호화하여 서버에 전달해야 한다.

Fisher 등은 이러한 문제점을 해결하고자 단일 게

이트 연산을 위임할 때마다 암/복호화하는 방식이 아닌 거의 모든 위임 게이트들을 서버가 계산하고 마지막에 양자 OTP 암호화된 양자 상태를 클라이언트가 복호화하는 암호화된 양자 상태 계산 기법을 제시하였다. Fisher의 양자 암호 기법은 제시한 모든 게이트 집합의 게이트가 OTP 암호화의 형태인 *Z*, *X* 게이트 순의 암호화 형태를 유지하도록 설계되었다. 위임 게이트를 적용할 때마다 양자 OTP 암호화 형태를 유지하지만, 양자 OTP의 키는 적용되는 게이트에 따라 바뀐다. 그러므로 클라이언트는 키 업데이트를 매번 수행하여 마지막에 클라이언트가 서버의 위임 계산이 적용된 양자 상태 결과를 복호화할 수 있다.

다. 연구 동향

2001년에 Childs가 제시한 위임 계산 프로토콜은 클라이언트가 양자 메모리를 가져야 하며 Two-qubit SWAP을 수행해야 하는 제약사항이 있다. 2006년 Arrighi와 Salvail는 범용 양자 계산이 아닌 특정 함수에 특화된 양자 비밀 계산을 지원하는 프로토콜을 제시하였다[4]. 2015년 Broadbent 등은 범용 양자 게이트 집합인 *X*, *Z*, *H*, *P*, *R*, *CNOT*에 대해 양자 비밀 계산을 지원하는 프로토콜을 제시하였다[5]. 2017년 Tan 등은 또 다른 범용 게이트 집합인 *H*, *P*, *CNOT*, Toffoli를 지원하는 양자 비밀 계산 프로토콜을 제시하였는데 해당 프로토콜은 입력과 결과 정보는 서버에 숨길 수 있지만, 계산식에 대한 정보는 숨길 수 없었다[6]. 2018년 Liu 등은 입력/결과뿐만 아니라 계산식도 서버에 숨길 수 있는 양자 비밀 계산 프로토콜을 제시하였다. Liu 등은 *H*, *P*, *CZ*, *CNOT*, Toffoli 범용 게이트 집합에 대해 비밀 계산을 지원하는 프로토콜을 제시하였다[7].

이상적인 양자 비밀 계산은 클라이언트에 요구되는 양자 계산 리소스가 최소화되어야 한다. 또한, 입력/결과 그리고 계산식 모두에 대한 정보 노출을 하지 않으면서 서버에 위임 연산을 수행할 수 있는 것이 이상적으로, 이를 목표로 이론적인 양자 암호 프로토콜 설계 연구가 진행되고 있다. 또한, 비밀 계산 프로토콜에서 필요한 서버와 클라이언트 간의 상호작용(Interaction)을 최소화하는 방안과 서버의 연산 결과에 대한 검증 또한 연구되고 있다[8,9].

2. 측정 기반 양자 비밀 계산

가. 범용 양자 비밀 계산(UBQC)

2009년 Broadbent 등은 측정 기반 양자 컴퓨팅 모델에서만 사용할 수 있는 범용 양자 비밀 계산(UBQC: Universal Blind Quantum Computation) 프로토콜을 제시하였다[10]. 측정 기반 양자 컴퓨팅 모델에서는 양자 계산이 측정방식에 따라 결정되기 때문에 양자 계산 과정을 클래식 컴퓨터로 처리할 수 있도록 구분 지을 수 있는 특징이 있다. 이러한 특징을 이용하여 양자 계산을 위한 측정 과정을 클래식한 암호화 방법으로 클라이언트가 서버로부터 정보 노출을 막는 것이 핵심이다. 회로 기반 양자 비밀 계산대비 측정 기반 양자 비밀 계산의 장점은 클라이언트의 양자 계산 요구사항이 줄어든다. 또한, 입력 데이터뿐만 아니라 계산에 대한 프라이버시 보호가

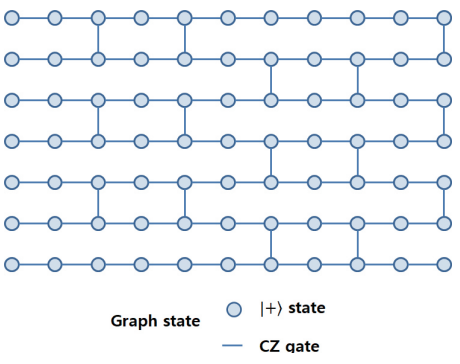

그림 7 Brickwork 양자 상태

가능하다. 단점은 측정 기반 양자 계산 특성상 더 많은 큐빗이 필요하다는 것이다.

범용 양자 비밀 계산 프로토콜의 전반적인 과정은 다음과 같다. 먼저 측정 기반 양자 계산의 준비과정에서 그림 7과 같이 Brickwork 양자 상태의 개별 큐빗을 클라이언트가 8개의 랜덤한 양자 상태 중 랜덤하게 선택하여 서버에게 준비시킨다. 다음으로 측정 기반 양자 계산의 진행과정에서 측정 베이시스를 클라이언트가 계산하여 서버에게 보내준다. 이때, 클라이언트는 준비과정에서 생성한 랜덤한 양자 상태를 고려하여 랜덤 정보를 상쇄시키고 의도한 측정 베이시스가 관측에 사용되도록 계산해서 서버에게 보낸다. 이는 의도된 측정 베이시스를 암호화하여 보내는 것과 같은 효과를 낸다. 서버는 측정 기반 양자 계산을 클라이언트가 요청한 대로 수행하지만 어떠한 양자 계산이 수행되고 있는지는 알 수 없게 된다.

2012년 Barz 등은 Broadbent 등이 제시한 측정 기반 범용 양자 비밀 계산 프로토콜을 실험적으로 입증하였다. Barz 등은 클라이언트가 Photonic 큐빗을 준비하고 전달할 수 있는 조건으로 측정 기반 범용 양자 비밀 계산 프로토콜을 적용한 Two-qubit Grover 알고리즘 계산을 수행하여 양자 비밀 계산을 실증했다[11].

나. 연구 동향

2013년 Morimae 등은 측정 기반 범용 양자 비밀 계산 프로토콜에서 서버와 클라이언트의 역할을 바꾼 방식으로 새로운 양자 비밀 계산 프로토콜을 제시하였다. 암호화된 스테이트 준비를 클라이언트가 수행하는 기존 방식과는 반대로 서버가 MBQC의 준비과정을 모두 수행하고 싱글 큐빗 측정을 클라이언트가 진행하여 계산을 수행하는 방식으로 서버는 계산에 대한 정보를 받지 않아서 계산에 대한 기밀성과 입/출력의 기밀성을 모두 보장한다[12].

Morimae 등이 제안한 방식은 서버가 MBQC의 준비과정을 고정된 방법으로 수행한다. 이점을 이용하여 스테빌라이저(Stabilizer) 게이트를 활용한 측정을 통해 서버가 준비과정을 제대로 수행했는지에 대한 검증을 효율적으로 수행할 수 있다는 장점이 있다.

양자 서버의 수를 늘리는 방식도 제안되었는데, 2013년 Reichardt 등은 양자 위임 계산 수행을 위한 양자 서버가 단일 서버가 아닌 둘 혹은 다수의 양자 서버가 위임 계산을 수행하는 양자 비밀 계산 모델을 제시하였다[13,14]. 다중 서버를 이용한 기법들의 제한사항은 서버 간에 초기 MBQC 셋팅에서 사용되는 큐빗이 얽힌 양자 상태를 가지고 진행해야 하며 서버 간의 공모 공격은 없다고 가정하는 것이다. 이러한 제한사항 아래에 클라이언트가 양자 컴퓨팅 능력이 전혀 없어도 양자 비밀 위임 계산을 수행할 수 있음을 보였다. 특히 CHSH 게임을 활용하여 프로토콜을 설계하여 두 개의 서버만으로도 완전한 클래식 클라이언트의 비밀 위임 계산이 가능함을 보였다[13].

2017년 Fitzsimons 등은 범용 양자 비밀 계산 기법에서 서버의 올바른 프로토콜 수행 여부를 검증하는 효율적인 방법을 제시하였다. 논리적 큐빗이 아닌 물리적 큐빗을 트랩 큐빗으로 이용하여 서버의 악의적인 동작을 효율적으로 탐지하는 검증 방법을 제안하였다[9].

Ⅴ. 결론

본고에서는 기본적인 양자 컴퓨팅과 다소 새로운 측정 기반 양자 컴퓨팅 모델을 살펴보고, 양자 컴퓨팅 서버와 고전 컴퓨팅 클라이언트 간의 프라이버시 보호 기능을 제공하는 양자 위임 계산에 관한 연

구 현황을 살펴보았다.

회로 기반 양자 컴퓨팅 모델에서는 암호화된 양자 상태에서 서버가 위임 계산을 진행하고 클라이언트가 복호화하여 원하는 결과를 얻는 모델로 동형 암호 활용 모델과 유사하다. 측정 기반 양자 컴퓨팅 모델에서는 측정에 사용되는 베이시스 정보를 클라이언트가 숨기면서 MBQC 계산을 서버와 함께 진행하여 계산식과 입출력에 대한 프라이버시를 보호하였다. MBQC 기반의 위임 비밀 계산은 계산식까지 숨길 수 있으며 서버의 무결성을 검증하는 등 높은 보안성을 제공하지만 많은 큐빗과 서버와 클라이언트 간 많은 통신이 필요하다는 단점이 있다.

프라이버시 보호 기능을 제공하는 안전한 양자 위임 계산 기술은 양자 컴퓨팅의 상용화와 보급을 가속할 수 있는 중요한 기술로서, 현재 활발한 연구가 진행 중이다. 양자 서버와 클래식 클라이언트 간의 안전한 위임 계산과 무결성을 보장하기 위한 다양한 방법이 제안되고 있으며, 이러한 연구는 양자 컴퓨팅의 실질적인 응용 가능성을 높이는 데 이바지할 수 있을 것으로 기대된다.

용어해설

CHSH 게임 두 명의 플레이어가 독립적으로 질문(x, y)을 받고, 사전 합의된 전략을 통해 $a \oplus b = x \cdot y$ 수식을 최대한 자주 만족시키는 게임으로, 고전적 방법보다 양자 얽힘을 활용할 때 더 높은 승률을 보임. 이 게임은 양자 얽힘과 벨 비대칭을 테스트하여 양자 물리학의 특성을 실험적으로 증명하는 도구로 사용됨

약어 정리

CNOT	Controlled-NOT(quantum gate)
MBQC	Measurement-Based Quantum Computation
OTP	One-Time Pad
UBQC	Universal Blind Quantum Computation

참고문헌

[1] A. Childs, "Secure assisted quantum computation," Quant. Inf. Comput. vol. 5, no. 6, 2005. pp. 456-466.

[2] A. Ambainis et al., "Private quantum channels," in Proc. 41st Annu. Symp. Foundations Comput. Sci., (Los Alamitos, CA, USA), 2000.

[3] K. Fisher et al., "Quantum computing on encrypted data," Nat Commun., vol. 5, 2014.

[4] P. Arrighi and L. Salvail, "Blind quantum computation," Int. J. Quantum Inform., vol. 4, no. 5, 2006, pp. 883-898.

[5] A. Broadbent, "Delegating private quantum computations," Can. J. Phys. vol. 93, no. 9, 2015, pp. 941-946.

[6] X. Tan et al., "Universal half-blind quantum computation," Ann. Telecommun., vol. 72, no. 9-10, 2017, pp. 1-7.

[7] W. Liu et al., "Full-blind delegating private quantum computation," Comput. Materials Continua, vol. 56, no. 2, 2018, pp. 211-223.

[8] A. Broadbent, "How to Verify a Quantum Computation," Theory Comput., vol. 14 no. 11, 2018, pp. 1-37.

[9] J.F. Fitzsimons and E. Kashefi, "Unconditionally verifiable blind quantum computation," Phys. Rev. A vol. 96, 2017.

[10] A. Broadbent, J. Fitzsimons, and E. Kashefi, "Universal blind quantum computation," in 50th Annu. IEEE Symp. Foundations Comput. Sci. (Atlanta, GA, USA), 2009.

[11] S. Barz et al., "Demonstration of blind quantum computing," Sci., vol. 335, no. 6066, 2012, pp. 303-308.

[12] T. Morimae and K. Fujii, "Blind quantum computation protocol in which Alice only makes measurements," Phys. Rev. A, vol. 87, 2013.

[13] W. Reichardt, F. Unger, and U. Vazirani, "A classical leash for a quantum system: Command of quantum systems via rigidity of CHSH games," arXiv Preprint, 2012, https://doi.org/10.48550/arXiv.1209.0448.

[14] W. Reichardt, F. Unger, and U. Vazirani, "Classical command of quantum systems," Nature, vol. 496, 2013, pp. 456-460.