# Blind Quantum Computation and Quantum Homomorphic Encryption: Foundations, Obstacles, and Capabilities

**CS 5134 Final Project**

Trevor Jarzynka
Virginia Tech
trevorj04@vt.edu

December 6, 2024

**Abstract**

This paper explores two foundational protocols in secure quantum computing: Blind Quantum Computation (BQC) and Quantum Homomorphic Encryption (QHE). These protocols aim to enable secure access to quantum computational power on untrusted servers. BQC ensures the privacy of data and computation by concealing all client information from the server, while QHE allows computations on encrypted data without revealing the data itself. The paper provides an overview of the underlying principles, mathematical foundations, and step-by-step methodologies for both protocols, compares their security, client and server requirements, resource needs, and application scenarios. The findings highlight their complementary roles in the advancement of secure and efficient quantum computing.

## 1. Introduction

Quantum computing has immense potential for solving complex problems that are currently infeasible for classical systems. However, the accessibility of quantum hardware is limited making secure remote computation on untrusted servers a critical area of research. Secure protocols such as Blind Quantum Computation (BQC) and Quantum

Homomorphic Encryption (QHE), provide solutions to this challenge by enabling computation without exposing sensitive data or computational processes to the server. This paper delves into the concepts, mechanisms, and comparative strengths of these protocols, highlighting their implications for quantum computing security and efficiency.

# 2. Protocol Details

### 2.1 Blind Quantum Computation (BQC) Details

BQC works on the following scenario: Alice wants to use Bob's quantum server to perform a quantum algorithm. Alice owns a small quantum device that can prepare single-qubit states, but she does not trust Bob with any secret information about her inputs or the computation steps.

1. Alice picks a sequence of random angles $[\theta_1, \theta_2, ..., \theta_n]$ and uses these to prepare qubits in states like

$$|\psi_{\theta i}\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{\theta_i i}|1\rangle)$$

Each $\theta_i$ is chosen randomly so Bob gains no information from these states.

2. Alice sends these encrypted qubits $|\psi_{\theta i}\rangle$ to Bob over a quantum channel

3. Alice wants Bob to perform a certain quantum algorithm. She communicates the type of gates to apply, but not the actual data of the input. Bob does not know the significance of these gates because the states are effectively masked by Alice's randomization.

4. After performing all requested operations, Alice instructs Bob to measure certain qubits in specified bases. For example, Bob performs the measurements and sends the classical results "Qubit 2 measured 0, Qubit 4 measured +" back to Alice.

5. Alice applies the inverse of the random rotations she did at the start to translate Bob's reported outcomes into the correct logical result of her intended computation

### 2.2 Quantum Homomorphic Encryption Protocol Details

QHE works on the following scenario: Alice wants Bob to perform a certain universal quantum computation on her data. She encrypts her qubits so that Bob can apply gates homomorphically.

1. Alice first encrypts her qubits using an encryption scheme that ensures secure ho-

momorphic computations. For example, the quantum one-time pad ***(Definition 2)***

2. Alice sends these encrypted qubits to Bob. She does not provide any information on how the qubits were encrypted to Bob so ensure Bob only sees what looks like random states.

3. Alice gives Bob instructions to implement a certain quantum circuit on the encrypted data.

- If the gates are Clifford gates, Bob can directly apply them, and Alice knows how these gates commute or anti-commute with the Pauli operators that form the encryption and she can decrypt the information.
- For non-Clifford gates, Alice might supply some auxiliary encrypted qubits and classical instructions so that Bob can still apply these gates without learning the key.

4. After finishing the computation, Bob sends the resulting encrypted quantum state back to Alice. He never decrypts or learns anything about the data or intermediate results.

5. Upon receiving the processed qubits, Alice applies the inverse of her encryption scheme to each qubit to recover the final state.

# 3. Protocol Analysis

## 3.1 Blind Quantum Computation (BQC)

The idea behind this protocol is to provide secure access to the advantages of quantum computing. This is achieved through the concept of blindness. In short, a protocol is blind if the server learns nothing about the client's input, output, and computation, except an upper bound on its size. The complete definition is:

**Definition 1 (Blindness)[BFK09]:** *Let $P$ be a quantum delegated computation on input $X$ and let $L(X)$ be any function of the input. We say that a quantum delegated computation protocol is blind while leaking at most $L(X)$ if, on Alice's input $X$, for any fixed $Y = L(X)$, the following two hold when given $Y$ :*
*1. The distribution of the classical information obtained by Bob in $P$ is independent of*

*X.*
*2. Given the distribution of classical information described in 1, the state of the quantum system obtained by Bob in P is fixed and independent of X.*

### 3.1.1 Blind Quantum Computation (BQC) Protocol Steps:

**Step 1. Client Quantum State Preparation**

The client prepares a set of qubits in specific quantum states encrypted using random parameters. These states are often randomly rotated qubits, such as $|+\rangle$ or $|-\rangle$ states rotated by angles $\theta_i$. This form of encryption prevents the server from gaining any information about the prepared states

**Definition 2 (Quantum One-Time Pad) [BFK09]:** *The quantum one-time pad is an encryption scheme where a quantum state $\rho$ is encrypted by applying a random Pauli operator, resulting in the state:*

$$\rho' = X^a Z^b \rho Z^b X^a$$

*where $a, b \in \{0, 1\}$ are random classical bits.*
To ensure this is secure quantum encryption scheme the outline of the proof principles is as follows:

1. Pauli operators form a basis $[I, X, Y, Z]$ form an orthogonal basis for $2X2$ matrices, so any single-qubit density matrix $\rho$ can be expressed in terms of

$$\rho = \frac{1}{2}I + \sum_{i \in \{x,y,z\}} r_i \sigma_i$$

where $\sigma_i$ are Pauli operators and $r_i$ are coefficients that satisfy $r_i^2 \leq 1$

2. When we consider all possible $a, b \in \{0, 1\}$, when averaged the random application of $X^a Z^b$ uniformly mixes the quantum state:

$$E(\rho) = \frac{1}{4} \sum_{a,b \in \{0,1\}} X^a Z^b \rho Z^b X^a$$

3. Each Pauli operator randomizes the state.

4. Because the random choices $a$ and $b$ are independent and uniformly distributed, the contributions from $[X, Y, Z]$ cancel out the off-diagonal terms in $\rho$ resulting in

$$\frac{1}{2}I$$

which is a completely mixed state that achieves perfect secrecy

**Step 2. Server Communication**
The client sends the encrypted qubits to the server over a quantum channel. The server acknowledges receipt and proceeds with the computation as instructed. The concept of a quantum channel is "*a mathematical model representing the physical processes that transmit quantum states from a sender to a receiver*". **[GIN18]**

**Step 3. Server Computation**
The server applies quantum gates and operations on the encrypted qubits per the client's instructions, without knowing the actual states.

**Theorem 1 (Universal Blind Quantum Computation) [F17]:** *Any quantum computation can be performed in a blind fashion such that the server learns nothing about the computation, provided the client can prepare specific single-qubit states.*

**Step 4. Measurement and Results**
After completing the computation, the server measures the qubits according to the client's instructions and sends the classical results back to the client. The client uses the initial random parameters to decrypt the results and obtain the final computation outcome.

### 3.1.2 Mathematical Foundation

**Quantum Encryption Foundation**
The client's qubits are in states:

$$|\psi_{\theta i}\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{\theta_i i}|1\rangle)$$

where $\theta_i$ are random angles. This ensures that any measurement by the server yields no information about $\theta_i$.

**Measurement-Based Quantum Computing**
Blind Quantum Computing often utilizes Measurement-Based Quantum Computing, where computation is performed through measurements on a highly entangled resource state.

**Theorem 2 (Blindness in MBQC) [GIN18]:** *Any quantum computation can be performed in a blind fashion such that the server learns nothing about the computation, provided the client can prepare specific single-qubit states.*

**Blindness**

The protocol's blindness is formalized by proving that the server's view is statistically independent of the client's private information.

**Definition 3 (Server's Viewpoint) [BFK09]:** *The server's view consists of the quantum states received, the operations performed, and the classical information exchanged during the protocol.*

## 3.2 Quantum Homomorphic Encryption: (QHE)

Quantum homomorphic encryption is a technique to perform computations on encrypted qubits. This protocol ensures that an untrusted server can implement a universal set of quantum gates on encrypted qubits without learning any information about the inputs. This heavily relies on the concept of homomorphic encryption which is defined as follow:

**Definition 4 (Homomorphic Encryption) [BJ15]**
*A homomorphic encryption scheme is a cryptographic system consisting of four algorithms: Key Generation, Encryption, Decryption, and Homomorphic Evaluation. It allows computations to be performed directly on encrypted data without requiring decryption. A scheme is fully homomorphic encryption if it supports operations for any circuit class and ensures compactness, meaning the decryption complexity is independent of the evaluated function's size.*

### 3.2.1 Quantum Homomorphic Encryption Protocol Steps

**Step 1. Client Encryption**

The client prepares and encrypts their quantum data using a quantum encryption scheme, such as the quantum one-time pad **(Definition 2)**.

**Step 2. Server Computation**

The server performs quantum computations directly on the encrypted data without decrypting it. This is possible due to the homomorphic properties of certain quantum gates, particularly the Clifford gates and specific non-Clifford gates when handled appropriately.

**Theorem 3 (Computations on Encrypted Quantum Data) [KBS+14]** *Quantum computations consisting of Clifford gates can be performed directly on data encrypted with the quantum one-time pad* ***(Definition 2)*** *, with the encryption keys being appropriately updated. For non-Clifford gates, additional techniques involving auxiliary qubits and limited classical communication are employed to enable computation without revealing the encryption keys.*

**Step 3. Client Decryption**

After the server completes the computation, the client receives the encrypted result. The client then decrypts the data using the encryption key (a,b) to obtain the final computation outcome.

### 3.2.2 Mathematical Foundation

**Quantum Encryption Technique**

The client's encrypted qubits are in states:

$$|\psi_{enc}\rangle = X^a Z^b |\psi\rangle$$

ensuring that, without knowledge of $a$ and $b$, the server gains no information about $|\psi\rangle$ can be gained.

**Definition 5 (Server's Viewpoint in QHE) [KBS+14]**

*The server's view consists of the quantum states received, the operations performed, and any classical information exchanged during the protocol.*

With the server's view not including any information about $a$ or $b$ the protocol is blind **(Definition 1)**.The security of the QHE protocol relies on the indistinguishability of encrypted states and the inability of the server to learn anything about the plaintext or the computation.

**Definition 6 (Security of QHE) [BJ15]**

A QHE scheme is secure if, for any two quantum plaintexts $\rho_0$ and $\rho_1$ and any quantum operation $U$, the server's view during the computation is indistinguishable between the two cases, in other words

$$View_{server}^{\rho_0} \approx View_{server}^{\rho_1}$$

**Theorem 4 (Security of the QHE Protocol) [KBS+14]**

*The QHE protocol provides information-theoretic security against an untrusted server, assuming perfect encryption by the client.*

The quantum one-time pad **(Definition 2)** ensures that the server's received states are maximally mixed which reveals no information about the plaintext. The protocols for non-Clifford gates prevent the server from learning the encryption keys or the computation details which ensures that QHE is a secure protocol.

**Homomorphic Properties of Quantum Operations**

Certain quantum gates commute or have predictable transformations with respect to

Pauli operators, allowing computations on encrypted data.

- **Clifford Gates** These gates either commute or anti-commute with Pauli operators, enabling direct computation on encrypted qubits. The encryption keys can be updated based on the gates applied.
- **Non-Clifford Gates** For gates like the $R$ gate, additional protocols involving auxiliary qubits are required.

**Theorem 5 (Universal Quantum Homomorphic Encryption) [KBS+14]**
*Any quantum computation can be performed homomorphically on quantum data encrypted with the quantum one-time pad* ***(Definition 2)****, provided appropriate protocols are used for non-Clifford gates*

For Clifford gates, the homomorphic property follows their relations with Pauli operators. For non-Clifford gates, protocols involving auxiliary qubits and classical communication ensure that the correct operation is applied without revealing the encryption keys

# 4. Comparison

Blind Quantum Computation (BQC) and Quantum Homomorphic Encryption (QHE) are foundational protocols designed to facilitate secure quantum computation on untrusted servers. These protocols play a critical role in the quantum computing landscape, enabling broader access to quantum computational power without requiring individuals or organizations to own quantum hardware. While both BQC and QHE share the common goal of protecting a client's data and computation from potentially malicious servers, they achieve this through distinct methodologies, offer different capabilities, and are suited for varying application scenarios.

## 4.1 Comparison of BQC and QHE

**Security**

***BQC:*** Ensures the privacy of both the data and the computation process. The server learns nothing about the client's input, output, or the specific computation being performed.

***QHE:*** Focuses on data privacy. The server can perform computations on encrypted data without learning about the input data, but the computation process itself is not hidden from the server.

**Client Requirements**

***BQC:*** The client must be able to prepare specific quantum states such as randomly rotated qubits and may need to interact with the server during computation for measurement instructions or other reasons.

***QHE:*** The client needs to perform quantum encryption and decryption but does not need to be involved during the computation phase on the server.

**Server Capabilities**

***BQC:*** The server operates under the client's instruction, performing computations on encrypted qubits without knowledge of their states.

***QHE:*** The server autonomously performs computations directly on encrypted data, leveraging the homomorphic properties of the encryption scheme.

**Resource Requirements**

***BQC:*** May require more communication between the client and server during computation, which can introduce overhead if performing interactive protocols.

***QHE:*** Reduces the need for interaction during computation, potentially leading to more efficient protocols in terms of communication complexity.

**Use Cases**

The use cases for Blind Quantum Computation (BQC) and Quantum Homomorphic Encryption (QHE) depend on the security requirements and resource constraints of the quantum system in question. Both protocols can be applied independently or in combination, depending on the desired level of security and the system's capabilities. In any scenario where security is a priority, these protocols should be carefully evaluated and integrated based on the specific needs of the application.

The decision to use BQC, QHE, or both simultaneously should be guided by the system's resource availability and the required security guarantees. Systems with ample resources might combine both protocols to achieve maximum security, while resource-limited systems might selectively implement one protocol depending on the context.

# 5. Conclusion and Open Questions

The study presents a comprehensive analysis of Blind Quantum Computation and Quantum Homomorphic Encryption, showcasing their distinct approaches to securing quantum computation on untrusted servers. BQC ensures complete privacy, making it ideal for sensitive computations, while QHE provides efficiency by enabling computations on encrypted data. Together, these protocols address key challenges in quantum computing, paving the way for broader adoption of secure and scalable quantum systems.

**Open Questions**

The security of quantum computations is a heavily studied field with a lot of open questions. Some of the open questions within these fields are as follows:

Can BQC and QHE protocols be combined with other quantum cryptographic techniques (quantum key distribution) for hybrid systems offering stronger guarantees?

How can these protocols be scaled? Are the resource requirements too much to implement these at scale?

Can classical post-processing be leveraged more effectively to reduce the quantum resources required on the client side?

How can we efficiently handle non-Clifford gates, which currently require additional resources and auxiliary qubits?

# References


[BFK09] A. Broadbent, J. Fitzsimons and E. Kashefi, "Universal Blind Quantum Computation," 2009 50th Annual IEEE Symposium on Foundations of Computer Science, Atlanta, GA, USA, 2009, pp. 517–526, doi: 10.1109/FOCS.2009.36.

[GIN18] L. Gyongyosi, S. Imre and H. V. Nguyen, "A Survey on Quantum Channel Capacities," in IEEE Communications Surveys & Tutorials, vol. 20, no. 2, pp. 1149– 1205, Secondquarter 2018, doi: 10.1109/COMST.2017.2786748.

[F17] J. Fitzsimons, "Private quantum computation: an introduction to blind quan-

tum computing and related protocols," npj Quantum Inf 3, 23 (2017), doi: https://doi.org/10.1038/s41534- 017-0025-3

[BJ15] A. Broadbent, and S. Jeffery, "Quantum homomorphic encryption for circuits of low T-gate complexity," Advances in Cryptology – CRYPTO 2015, vol. 9216, pp. 609–629, 2015, doi: https://doi.org/10.1007/978-3-662-48000-7_30

[KBS+14] K. Fisher, A. Broadbent, L. Shalm, et al. "Quantum computing on encrypted data," Nat Commun 5, 3074 (2014). doi: https://doi.org/10.1038/ncomms4074