Implementing CCZ Gates with Variation of Gate Teleportation for Quantum Homomorphic Encryption on NISQ Platform

1st Gia Phat Dang
Western Sydney University
Sydney, Australia
0009-0006-4903-0376
22040062@student.westernsydney.edu.au

2nd Weisheng Si
Western Sydney University
Sydney, Australia
0000-0002-1239-7880
W.Si@westernsydney.edu.au

3rd Belal Alsinglawi
Zayed University
Abu Dhabi, U.A.E
0000-0003-0316-3641
Belal.AlSinglawi@zu.ac.ae

4th Jim Basilakis
Western Sydney University
Sydney, Australia
0000-0002-7440-1320
J.Basilakis@westernsydney.edu.au

***Abstract*—While quantum computing technologies are revolutionising key industries, distributed quantum hardware services are dominated by quantum providers such as IBM, Google, and AWS. It raises critical data security concerns across sectors such as banking, defence, and healthcare. To address this issue, Quantum Homomorphic Encryption (QHE) has emerged as a solution that enables computations on encrypted quantum data while preserving privacy. Despite its promise, deploying QHE remains challenging due to circuit complexity and the noise in today's quantum systems. In this work, we confront these barriers directly by implementing QHE on Noisy Intermediate-scale Quantum (NISQ) devices using the Variation of Gate Teleportation (VGT) scheme. In particular, we focus on implementing the CCZ gate, a key non-Clifford gate that makes a quantum gate set universal when combined with Clifford gates. By leveraging the techniques from the Classical Quantum Circuit (CQC)-QHE framework proposed by Ortega et al. in 2025, our implementation reduces computational cost and improves resource efficiency. As a result, our approach can support 7 qubits and 14 T-gates in the circuit without large errors, improving on existing QHE implementations.**

***Index Terms*—Quantum Cloud Computing (QCC), Quantum Homomorphic Encryption (QHE), Classical Quantum Circuit (CQC), Noisy Intermediate-scale Quantum (NISQ), Controlled-Controlled-Z (CCZ), Variation of Gate Teleportation (VGT)**

I. Introduction

The constraints of quantum communication and hardware, such as quantum memory, have led to the emergence of hybrid classical and quantum systems known as a Quantum Cloud Computing (QCC) [1]. This concept enables the remote use of quantum hardware to analyse large datasets or execute complex algorithms. In recent years, hybrid quantum-classical cloud systems have become popular for solving real-world problems, particularly in sensitive fields such as finance, defence, and healthcare [2]–[4]. However, the immaturity of current noisy quantum devices, combined with the specific requirements of quantum physicists within classical frameworks, presents challenges in achieving high accuracy and robust security [5]. In the current QCC environment, QHE is proposed as a promising security solution that enables users to outsource the processing of encrypted data to a quantum server [6]. In the hybrid QCC models, the practicality of QHE schemes requires no interaction between the client and the server, a property called non-interactive QHE algorithms [7].

To effectively develop the practical QHE, called as Quantum Fully Homomorphic Encryption (QFHE) schemes, three main conditions must be met: universal computation, perfect theoretical security, and a compact decryption process [8]. However, the no-go theorem in quantum physics renders the simultaneous achievement of all three conditions impossible, resulting in exponential overhead for non-interactive QHE algorithms [9]. In the non-interactive QHE schemes, non-Clifford (T-gate or triple-qubit gates) operations are the main cause of algorithmic overhead due to an unexpected phase error. Since 2015, Broadbent has introduced a foundational Einstein-Podolsky-Rosen (EPR) evaluation scheme to handle this error. The approach uses teleportation-based Bell states to achieve square sublinear decryption complexity (L^2-quasi-compactness), where L is the number of T-gates, scaling with the square of the number of non-Clifford (T) gates in the EPR evaluation

Accepted for publication in the Proceedings of the 2026 IEEE International Conference on Quantum Control, Computing and Learning (IEEE qCCL2026) at Aalborg University, Aalborg, Denmark.

© 2026 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other publications.

circuit [10]. In 2024, Ganjian demonstrated the EPR in a local computer simulation using IBM-Qiskit, achieving maximum performance with 1 qubit and 6 T-gates, with a runtime of over 86 minutes [11].

Back in 2020, Liang proposed an optimal quasi-compact (L-quasi-compact) QHE framework that leverages a teleportation-based Bell concept, which reduces the decryption complexity from square sublinear (L^2) to sublinear scaling (L), called Variation of Gate Teleportation (VGT) (VGT-QHE) [7]. This reduction in decryption overhead is a key achievement of the VGT scheme, which is widely applied in many QHE publications, such as the integration of Grover's algorithm, the optimisation of the quantum ciphertext dimension, and the combination with the recursive Bernstein-Vazirani framework [12]–[14]. In 2025, Ortega et al. proposed a semiclassical (Classical Quantum Circuit (CQC)-QHE) simulation framework (or circuit formalism) that enables sequential evolution between classical and quantum stages, permitting intermediate measurements and reset operations during non-Clifford evaluation and decryption in VGT [15]. The execution of VGT in CQC provides a simulation threshold of 20 qubits (6 computational qubits) and a 7-T gate circuit [7], [15]. Despite theoretical advances while progressing from EPR to VGT evaluation, the NISQ experiment remains a critical factor for assessing the practicality of QHE, which has not been addressed in previous contributions [14].

In discussions of quantum advantage, Controlled-Controlled-Z (CCZ) is better described as a three-qubit gate primitive that can enable more resource-efficient quantum circuits [16]. It belongs to the non-Clifford group and enables multi-qubit entanglement. CCZ gates offer computational advantages for universal quantum computation and play a vital role in various quantum algorithms. However, the implementation overhead of CCZ decomposition on quantum hardware poses significant challenges when combined with the complexity of the universality QHE evaluation process. To address this gap, this paper presents a comprehensive QHE scheme, called (CCZ-QHE), that evaluates the CCZ gate. Additionally, the hardware implementation of the CCZ-QHE algorithm can provide insight into the behaviour of this secure quantum computation protocol in an NISQ environment, which identifies algorithmic weaknesses to support further development. This work provides three primary research contributions:

- We present CCZ-QHE, a scheme that homomorphically evaluates the three-qubit CCZ gate on encrypted quantum states.
- Our approach provides the first hardware validation of multi-qubit non-Clifford QHE on IBM Quantum processors, identifying practical fidelity limits under NISQ conditions.
- We evaluate the effectiveness of Pauli Twirling (PT) as a Quantum Error Mitigation (QEM) strategy for CCZ-QHE, establishing conditions under which error mitigation provides measurable improvement.

The research paper first describes relevant definitions and background for the CCZ-QHE scheme in Section 2. Section 3 presents the scheme and operational procedure for evaluating CCZ gates for QHE. Section 4 presents comprehensive implementation results in both local simulation and current NISQ mode. Finally, Sections 5 and 6 discuss the algorithm's feasibility and its weaknesses, and point out future research directions.

II. Background

A. General QHE architecture

Huang et al. propose that the general QHE architecture begins with the client employing Quantum One-Time Pad (QOTP) encryption to obscure quantum states by randomly applying Pauli operators (X^a and Z^b) to their states $|\psi\rangle$ [17]. Subsequently, the server performs a homomorphic evaluation of the encrypted state after applying Clifford and non-Clifford group gates, thereby ensuring security by blindly implementing the key-update mechanism [18].

The key tracking function not only influences the actual computational operation ($|\psi\rangle \rightarrow U|\psi\rangle$) but also alters the encryption pattern. Clifford gates H, X, Z, CNOT provide straightforward deterministic methods based on the key-update rule [10]. In contrast, non-Clifford gates introduce unknown phase errors that affect the accuracy of the decrypted result, due to Knill's theorem [19]. To solve the T-gate accumulative error, the client employs the computed final keys (a', b') to track all key transformations. These keys are used to decrypt the initial quantum state by inverting the Pauli operation $(Z^{b'}X^{a'})$ [17]. Although the EPR-QHE scheme can address this unexpected phase error at each T-gate [10], it imposes exponential overhead in decryption to $O(L^2)$ [11].

B. Gate Teleportation for Non-Clifford Gate's Evaluation

Since 2020, Liang has introduced a VGT evaluation method based on the $EG[P^x]$ protocol, overcoming the quadratic-scaling limitation of the EPR-QHE. Liang's framework sequentially performs key updating on-demand computation, acquiring O(n) bits as the number of keys stored. As a result, it enables reducing decryption complexity to $O(L_n \times log_2 n)$ calculations (with L = T-gates and n = qubits), reaching optimal M-quasi-compactness [7]. Nevertheless, Liang's VGT practically faces an exponential overhead at the number of key values because these keys are required to be pre-generated during $T/T\dagger$'s error correction by utilising the classically controlled S gates [14], [20]. Ortega has introduced a formalism for Liang's VGT decryption concept, called CQC. It allows the client to dynamically update keys during decryption by combining classical and quantum operations sequentially [15]. Additionally, Ortega introduces the semi-classical extension that

enables immediate measurement and reset execution, reducing the need to pre-generate all possible measurement results and transforming exponential overhead into $O(L)$ scaling with circuit size. Although the CQC-QHE algorithm successfully simulates 77 T-gates on Qiskit's local simulator, it is not hardware-feasible [15].

C. CCZ Decomposition Feature

Three-qubit gates (such as CCZ or Toffoli/CCX) are crucial for quantum universal computation, providing the advantages that distinguish quantum computations over classical methods [21]. The CCZ gates are popular, emerging in two major applications: algorithmic development (Grover's algorithm, Quantum Approximation Optimisation Algorithm (QAOA)) and fault-tolerant architectures (QEC code-based) [22], [23]. The CCZ gate acts on one target qubit according to two control qubits, implementing a phase flip of (-1) on the target qubit only when both control qubits are in the state $|1\rangle$. Note that if the target qubit has a state of $|0\rangle$, the phase flip is meaningless. Thus, we can also say that the CCZ gate applies a phase flip to the target qubit only when all three qubits are in the state $|1\rangle$. This operation can be expressed as:

$$CCZ\,|abc\rangle = (-1)^{(a\cdot b\cdot c)}\,|abc\rangle\,,$$

with $a, b, c \in 0, 1$.

According to Akahoshi et al., 7 T-gate and Clifford operations are the decomposition ideal for CCZ gates, which could affect the QHE computational budget due to scaling phase errors in homomorphic evaluation. As a result, evaluating CCZ gates in QHE schemes may be limited by computational noise introduced by handling T-gates because of CCZ's decomposition feature. Notably, IBM Quantum reports higher cumulative error when synthesising CCZ gates from Clifford and T-gates than when using T-gates alone [24]. For instance, Toffoli gate decomposition requires 6-9 CNOTs and 7 T-gates, yielding 56–63% fidelity, which is much lower than the 99% associated with Clifford+T implementations. These findings emphasise the need for rigorous T-gate management in triple-qubit gates [25].

D. Error Mitigation on NISQ Hardware

In current-generation NISQ hardware, algorithmic accuracy is affected by two significant errors: uncontrolled interaction between the qubit and the noisy hardware environment (incoherent) and a predictable systematic problem that accumulates over successive operations in the gate implementation (coherent) [26], [27]. Quantum Error Correction (QEC) requires substantial resources to dynamically correct errors on qubits, resulting in significant computational overhead in current NISQ systems. Given the complexity of Non-Clifford error in CCZ-QHE, limited NISQ resources pose a serious challenge to algorithmic feasibility, especially for the gate teleportation approach, the mid-circuit measurement method, and the SWAP operation on each T-gate. In contrast, QEM focuses on post-processing and circuit-level interventions, which are better suited to the constraints of quantum hardware. Among QEM techniques, the PT protocol has become popular for improving algorithmic accuracy. It targets the reduction of cumulative physical errors by applying randomly sampled Pauli conjugations and depolarising noise, which transform these errors into stochastic Pauli errors [28]. In QHE, the specific structure of the PT protocol ensures compatibility with the Pauli key-updating mechanism of QOTP and manages accumulative errors of non-Clifford groups by converting them into controllable Pauli noise.

III. Related Work

According to Figure 1, the **CQC-QHE** section shows Ortega et al.'s approach as distributed T-gates over distinct qubits (q_1, q_2, q_3) in the quantum Szegedy walk circuit. Each T-gate independently activates its teleportation gadget and the key-updating mechanism (k_1, k_2, k_3 or k_4). If a measurement yields incorrect key values, it only affects the affected qubit's key pair, leaving other qubit operations unaffected. In contrast, decomposing the CCZ gate uses 7 T/T† gates, applied sequentially to 3 qubits and interleaved with CNOTs (CX), illustrated in **CCZ-QHE** section of Figure 1. Thus, homomorphic CCZ evaluation creates a dependency chain across operations. Measurement results update the encryption key during T-gate correction and serve as direct inputs to the next operation on the same qubit. If a single point within the dependency chain collapses, it will cascade the rest. As a result, evaluating CCZ in a noisy quantum hardware environment poses compositional challenges that affect algorithmic accuracy, as it exposes actual behaviour and readout errors at each phase.

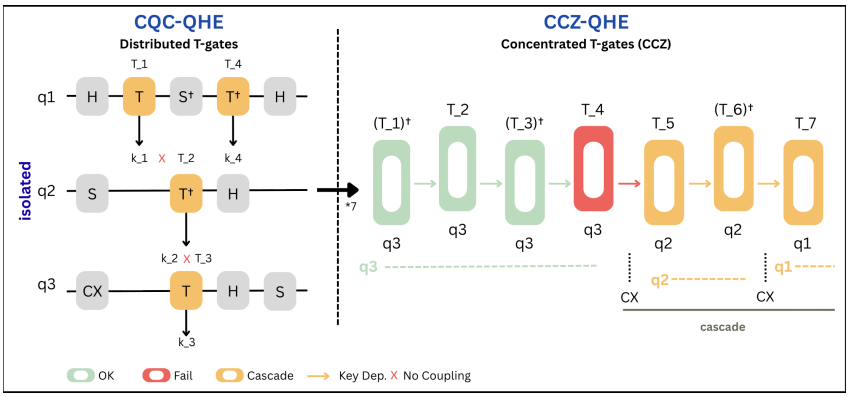
Based on the above discussion, we identify the critical factor of CCZ gates in quantum algorithms across various applications. Moreover, the most recent QHE-CQC implementation provides a high potential for evaluating extensive resources. These findings raise the gap in the practicality of QHE with CCZ evaluation.

IV. Methodology

A. Protocol Overview

To bridge the gap, our paper suggests implementing the CCZ gate within QHE, as described in Algorithm 1. The demonstration outlines four major phases of the CCZ-QHE, based on Ortega's work and the CCZ decomposition guidelines. First, Phase 1 encrypts the initial quantum state using QOTP. In Phase 2, the server performs homomorphic evaluation in response to the client's requested computation, while a key-updating process maintains the security of client information. In Phase 3, responsibility shifts back to the client to decrypt and recover the initial data, using classical controlled Bell measurement techniques to reverse key

Fig. 1: Differences between the CQC-QHE and CCZ-QHE schemes



Algorithm 1 QHE-CCZ Protocol

Require: Input state $|\psi\rangle$, gate sequence $\mathcal{G}$
Ensure: Decrypted output state
— Phase 1: Client Encryption (QOTP) —
1: Allocate registers: problem[n], bell[$2T$], ancilla[3]
2: Prepare $|\psi\rangle$ based on circuit type
3: $(x_k, z_k) \leftarrow \text{Rand}(\{0,1\}^n)$ ▷ Random QOTP keys
4: **for** $i = 0$ to $n-1$ **do**
5: **if** $x_k[i] = 1$ **then** $X(i)$
6: **end if**;
7: **if** $z_k[i] = 1$ **then** $Z(i)$
8: **end if**
9: **end for**
— Phase 2: Server Homomorphic Evaluation —
10: idx $\leftarrow 0$
11: **for** gate $g \in \mathcal{G}$ **do**
12: **if** $g \in \{H, X, Z, S, \text{CNOT}\}$ **then** Apply g directly
13: **else if** $g = T$ on qubit q **then** ▷ Gate teleportation
14: $a \leftarrow$ bell[idx]; $b \leftarrow$ bell[idx+1]
15: $H(a)$; CNOT(a, b); $T(a)$; CNOT(q, a); $H(q)$
16: $(r_a, r_b) \leftarrow \text{Measure}(q, a)$
17: **if** $r_a = 1$ **then** $X(b)$
18: **end if**;
19: **if** $r_b = 1$ **then** $Z(b)$
20: **end if**
21: SWAP(q, b); idx $\leftarrow$ idx $+2$
22: **else if** $g = \text{CCZ}(c_1, c_2, t)$ **then** ▷ 7-T decomposition
23: Apply optimal CCZ decomposition with teleportation
24: **end if**
25: **end for**
— Phase 3: Client Decryption —
26: **for** each shot in memory **do**
27: $(x, z) \leftarrow (x_k, z_k)$
28: **for** (gate, qubits) in sequence **do**
29: H: swap$(x[i], z[i])$; S: $z[i] \oplus= x[i]$
30: CNOT: $x[t] \oplus= x[c]$; $z[c] \oplus= z[t]$
31: T: $x[i] \oplus= r_a$; $z[i] \oplus= x[i] \oplus r_b$
32: **end for**
33: $m_{\text{dec}}[i] \leftarrow m_{\text{enc}}[i] \oplus x[i]$ ▷ Final decryption
34: **end for**
35: **return** decrypted measurement outcomes

updates and verify consistency with the homomorphic evaluation.

B. Resource Requirement

Figure 2 shows that the CCZ-QHE algorithm uses three types of quantum registers. The quantum resource register is estimated by the formulation: $n + 2T + 3$, where n is the number of data qubits, T is the number of T-gates, and 3 represents ancilla qubits needed for CCZ decomposition. Data qubits and T-gates define computational capability, while the ancilla qubits support the combined CQC-VGT techniques, highlighting the overhead from the full CCZ-QHE circuit.

C. QOTP Algorithm

Similar to the general QHE framework, our blind quantum cryptographic system utilises QOTP for initial encryption. In Phase 1 (lines 1 to 9), once quantum register allocation and initial state preparation are complete, the client generates two random n-bit keys $(x_{key}, z_{key} \in [0,1]^n)$. These random keys are subsequently used by QOTP to encrypt the prepared quantum states, producing the encrypted state $\left|\tilde{\psi}\right\rangle$. This resulting encrypted state is then transmitted to the server for homomorphic evaluation.

D. Homomorphic Evaluation Algorithm

Homomorphic evaluation is the most computationally intensive phase of the QHE-CCZ model, as it enables computation over encrypted states. In Phase 2 (lines 10-25), Clifford (H, X, Z, CNOT) and non-Clifford (T and CCZ) evaluations are performed separately to reduce computational complexity and optimise key traceability throughout the evaluation.

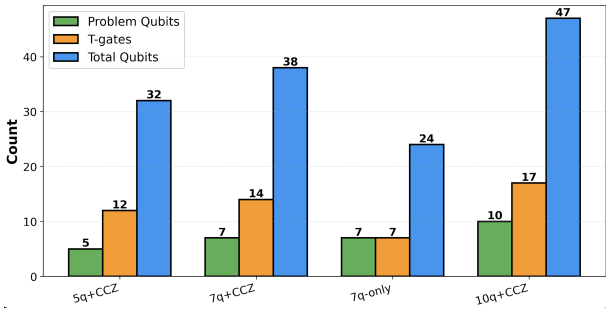
The Clifford key updating rules can simplify this step. However, undesirable phase errors arise from the interaction between QOTP encryption and non-Clifford gates (T-gate and CCZ gate) [10]. The algorithm addresses this by generating a Bell pair using the VGT-QHE framework (lines 14-15). The server then applies a T gate to a Bell qubit and executes a Bell-basis measurement. This includes CNOT, H, and measurement of both the problem and the Bell qubit. After measurement, the qubit state collapses, but the client can still receive a Bell qubit with the applied T-gate. To identify and correct the phase error, the server performs conditional Pauli corrections on the measurement result (r_a, r_b) (line 16). The server also entangles the SWAP state back to the problem qubit. The procedure utilises 24 Bell qubits for 12 T-gates, with one Bell pair assigned to each T-gate. In addition,

the CCZ decomposition process orchestrates 7 T-gates and 6 CNOT gates using alternating $T/T^\dagger$ layers and key updates for each CNOT operation (lines 22- 25).

E. QOTP Decryption Algorithm

Phase 3 (lines 28 - 34) illustrates the decryption process for recovering the evaluated computational states to their original form. The process begins with the server providing the encrypted measurement to the client. With the Clifford group, the client then performs per-shot decryption using a classical key-updating procedure provided by the server. On the other hand, the T-gate requires precise Bell-basis measurement outputs (r_a, r_b) per shot; this forms the measurement-extraction approach, which is crucial for T-gate key updating. Once the server concludes the key evolution process, the client receives the encrypted measurement bitstring (m_{enc}) and independently decrypts each shot m_{dec}. The decryption is performed via $b_{dec}[i] = b_{enc}[i] \oplus x[i]$, where $\oplus$ is the XOR operation. Notably, the Z_{key} is absent in this step because its global phase impact has no correspondence to the computational basis measurement.

Fig. 2: CCZ-QHE Configuration Summary



V. Experimental Results

A. Experimental Setup

The CCZ-QHE algorithm is generated by the Qiskit IBM Quantum SDK on a MacBook M3 with 36 GB of RAM. Hardware execution is performed on the IBM Quantum backend `ibm_marrakesh`, which has 156 qubits and 1024-shot measurement, including 99.95% two-qubit gate fidelity and 98% readout fidelity. Figure 2 presents four test configurations in sequence: (1) 5 qubits + CCZ, (2) 7 qubits + CCZ, (3) 7 qubits alone, and (4) 10 qubits + CCZ gate. Each configuration applies Clifford gates and a single T gate after each qubit. The algorithmic circuits are then structured according to the formula (Total Qubits = $n + 2T + 3$), which provides a general structure for universality in quantum computation.

B. Simulator Accuracy

We use the Qiskit Aer Simulator (with 1024-shot measurements) to deploy the QHE-CCZ architecture, simulating quantum features within a local simulation environment. As shown in table I, simulation fidelity metrics (F_{sim}) report an F value above 0.99, indicating nearly ideal algorithmic correctness. This high accuracy confirms all algorithm phases, including the CCZ decomposition (with non-Clifford evaluation) and the decryption logic. Analysis of the observed entropy reveals a uniform distribution of values across quantum states during QHE, confirming the security of QOTP encryption and decryption and ensuring no state collapse during T-gate evaluation. The $7q$+CCZ test case has the longest runtime because it uses the most complex circuit: 7 qubits and a CCZ gate. In contrast, the $10q$+CCZ test case requires 47 qubits according to the QHE-CCZ resource formula, which requires about 2.25 petabytes of memory ($2^{47} \times 16$ bytes), more than the local simulation environment can provide.

TABLE I: Scalability and QEM Effectiveness

Metric	5q+CCZ	7q+CCZ	7q-only	10q+CCZ
Runtime	22.8s	28.3s	11.7s	92.2s
F_{Sim}	0.998	0.997	0.999	N/A
F_{Raw}	0.9394	0.9243	**0.9652**	0.5350
F_{QEM}	**0.9523**	0.9185	0.9613	*Failed*
Entropy	0.995	0.982	0.988	0.978

C. Algorithm Performance on IBM-Hardware

Table I shows the total number of qubits, T-depth, and running time to measure how the algorithm scales. Raw fidelity (F_{Raw} - without QEM) and QEM-corrected fidelity (F_{QEM}) to validate the algorithmic performance on quantum hardware. For the 7q, 5q-CCZ, and 7q-CCZ test cases, the raw-fidelity values indicate algorithmic feasibility, as they remain above 60%. However, in the 10q-CCZ case, fidelity drops below 60%, indicating the algorithm is impractical. For example, raw fidelity drops from $F = 0.9652$ (7q-only) to $F = 0.5350$ (10q+CCZ). This decrease indicates that increasing the T-gate count, particularly in CCZ-decomposed cases, reduces fidelity more than adding qubits alone. Moreover, the increase in resources is 43% more qubits and 21% more T-gates as the problem size grows from 5 to 10 qubits. This result matches the expected scaling of quantum resources for the CCZ-QHE algorithm. Comparing $5q$+CCZ (32 total qubits, $F = 0.9394$) to $7q$-only (24 total qubits, $F = 0.9652$) shows that $5q$+CCZ, which has more qubits and a higher T-gate count, exhibits lower fidelity. Thus, differences in T-gate and problem qubit scaling have distinct effects on fidelity, with non-Clifford gates proving most detrimental. Applying the PT method, 5q+CCZ shows a 1.4% gain in fidelity. In contrast, both 7-qubit tests lose some accuracy, with a 0.6% drop (0.9243 to 0.9185) for 7q+CCZ and a 0.4% drop (0.9652 to 0.9613) for 7q-only. The 10-qubit case does not improve with PT, giving an 'IBM Internal Compiler Error 6053'.

TABLE II: Error Source Decomposition

Error Source	5q+CCZ	7q+CCZ	7q-only	10q+CCZ
Total error	**4.8%**	**7.6%**	**3.5%**	**46.5%**
CX gate count	∼180	∼250	∼120	∼600
Gate error est.	3.2%	4.8%	2.1%	>15%
Measurement count	∼50	∼70	∼35	∼120
Meas. error est.	1.5%	2.1%	0.9%	>5%
SWAP operations	∼20	∼35	∼15	∼100
Transp. error est.	0.8%	1.2%	0.5%	>3%

D. Error Decomposition and Algorithmic Noise Mechanism

Table II summarises the essential noise analysis across three major sources. Firstly, the total gate errors highlight the QEM fidelity failure rate relative to the ideal correctness, with the highest failure rate observed in the $10q$+CCZ case. Secondly, for the hardware transpilation circuit, error component metrics include CX gate count (IBM Quantum's transpilation), which shows over 600 additional gates after the transpilation at $10q$+CCZ and only 120 additional gates at $7q$-only. Finally, measurement error and the SWAP operation facilitate the Bell measurement used to evaluate the T-gate. Consistent with the other two noise analysis metrics, the T-gate error values show increases in the SWAP operation and measured error, respectively, from 0.8% to over 3% and from 1.5% to over 5%. This experiment yields a significant improvement in decomposed error over the $10q$ configuration.

VI. Discussion

This paper's experimental findings clarify the impact of T-gate dominance on algorithmic practicality, identify error factors in NISQ hardware implementation, and present a viable strategy to bridge the gap between simulation and implementation.

A. Impact of T-gate on the algorithm's practical threshold

First, Bell-pair preparation (via CX gates), mid-circuit measurement, and SWAP operations introduce three error sources that occur concurrently with each T-gate correction. The accumulation of 14 to 17 T-gates results in an exponential increase in key-update dependency chains, effectively degrading high-fidelity results into unusable QHE outputs. Furthermore, additional T-gates increase SWAP and CX gate counts, indicating a compounded effect driven by decoherence, circuit complexity, depth, and routing overhead. Consequently, the T-gate constitutes the primary bottleneck and establishes a practical threshold beyond which fidelity drops below acceptable levels. Our experiments indicate this threshold lies between 7 and 14 T-gates. These practical threshold metrics—combining T-gate count, problem qubits count, and hardware topology—serve as a proof of concept for real-world quantum computation operating within observed fidelity limits. Given the failure of the 10-qubit CCZ configuration, several enhancement strategies at different levels merit consideration: algorithm-level optimisations (e.g., reducing circuit complexity through parallelised T-gate execution), protocol-level innovations (e.g., employing T-gate magic states to improve Bell-pair measurement fidelity), and QEM techniques.

B. Algorithmic Feasibility Boundary

The CCZ-QHE framework handles small quantum circuits with up to 14 T-gates, including a 3-qubit Grover search (2 CCZ gates, 14 T-gates) and 2-layer nonlinear quantum classifiers. However, this threshold serves only as a proof of concept; real-world algorithms requiring multiple Grover iterations or 3-qubit gate rounds often exceed this limit. Extending the threshold to 30–40 T-gates is essential for practical applications. Regarding error mitigation,QEM methods such as PT introduce additional gates into the circuit but provide an enhancement only for the smallest (5-qubit + CCZ) configuration, which explains the observed scaling challenges on IBM Quantum hardware.

C. Comparison of the experiment result among CCZ-QHE scheme to other QHE variant

Table III illustrates the distinction between our implementation and earlier QHE papers, which use four majority metrics. In terms of computational resources, our CCZ-QHE implementation has the largest number of qubits, with 7. However, the universality of non-Clifford gates is lower than that of Ortega et al.'s work. This limited number of $T/T^\dagger$ is due to the noisy environment of quantum hardware compared with the ideal measurement environment of the CQC installation. Nevertheless, our implementation demonstrates the feasibility and meaningful progress of QHE algorithms for NISQ systems, highlighting their practical value for advancing secure quantum computation.

D. Security Under NISQ hardware

The local simulation environment of the CCZ-QHE scheme achieves near-ideal fidelity and maintains high-entropy measurement metrics, thereby strengthening the security of the CCZ-QHE protocol by leveraging the information-theoretic security of QOTP. The CCZ-QHE framework provides perfect security by building on Liang's scheme and leveraging a maximally mixed state via QOTP encryption. The extension via the CCZ gate maintains this security by fully decomposing into $T/T^\dagger$ and the Clifford group. While Liang's analysis and Ortega et al.'s framework assume ideal conditions, our hardware entropy measurements (0.982-0.995) confirm that QOTP encryption remains sound on IBM Quantum devices, as the predominantly depolarising noise channels (reinforced by PT converting coherent errors into stochastic Pauli errors) map states toward a maximally mixed state, preserving rather than compromising ciphertext randomness.

On the client side, the security concern shifts to decryption correctness: the 5q+CCZ and 7q+CCZ

TABLE III: Comparison between performance of CCZ-QHE implementation with other QHE variants

Metric	Ganjian et al. [11]	Fernández et al. [13]	Ortega et al. [15]	This Work (QHE-CCZ)
Number of Qubits	1 (Qiskit sim.)	3 (Qiskit sim.)	Up to 6 (Qiskit sim.)	**5, 7, 10** (IBM Quantum hardware)
Non-Clifford Gate Scope	$T/T^\dagger$ only	Toffoli	MCX	**CCZ**
Max T-gates Validated	6 (sim.)	7 (sim.)	$\sim$77 (sim.)	**17 on hardware** (5q:12, 7q:7–14, 10q:17)
Execution Platform	Qiskit simulation	Qiskit simulation	Qiskit simulation	**IBM Quantum**

configurations maintain acceptable fidelities ($F_{Raw} = 0.9394, 0.9243$; $F_{QEM} = 0.9523, 0.9185$), but degradation to $F_{Raw} = 0.5350$ at 10q+CCZ reveals that beyond the 14 T-gate threshold, error accumulation undermines utility while confidentiality is preserved. Implementing QHE on hybrid cloud platforms requires Fully Homomorphic Encryption (FHE) integration to safeguard QOTP-encrypted keys, shifting the security model from information-theoretic to semantic security (IND-CPA) under lattice-based assumptions.

VII. Conclusion

Integrating QHE protocols with broader quantum algorithms remains challenging, particularly in the NISQ era, where protocols must simultaneously satisfy cryptographic correctness and circuit-level resource efficiency. Motivated by the central role of the CCZ gate in many quantum algorithms, we implemented and evaluated a CCZ-QHE scheme on IBM quantum hardware, identifying a practical operating threshold of 7 qubits and 14 T gates. Experimental results highlight stochastic noise effects in current NISQ devices and indicate that T-gate cost dominates performance degradation, compounded by CX(CNOTs) overhead, intermediate measurements, and SWAP operations. Future work should focus on extending qubit and T-gate thresholds through improved compilation, key-update optimisation, and error-aware protocol design. This work establishes a practical baseline for CCZ-enabled QHE under realistic NISQ constraints and provides an evidence-based foundation for scalable, hardware-tailored quantum cryptographic protocols.

References

[1] M. Golec, E. S. Hatay, M. Golec, M. Uyar, M. Golec, and S. S. Gill, "Quantum cloud computing: Trends and challenges," *Journal of Economy and Technology*, vol. 2, pp. 190–199, 2024.

[2] M. SaberiKamarposhti, K.-W. Ng, F.-F. Chua, J. Abdullah, M. Yadollahi, M. Moradi, and S. Ahmadpour, "Post-quantum healthcare: A roadmap for cybersecurity resilience in medical data," *Heliyon*, vol. 10, no. 10, 2024.

[3] A. Zafar, "Quantum computing in finance: Regulatory readiness, legal gaps, and the future of secure tech innovation," *European Journal of Risk Regulation*, pp. 1–32, 2025.

[4] S. Ali, S. A. Wadho, K. R. Talpur, B. A. Talpur, K. S. Alshudukhi, M. Humayun, S. R. Talpur, M. A. Al Mamun, M. Naseem, A. Abro *et al.*, "Next-generation quantum security: the impact of quantum computing on cybersecurity—threats, mitigations, and solutions," *Computers and Electrical Engineering*, vol. 128, p. 110649, 2025.

[5] R. Ramya, P. Kumar, D. Dhanasekaran, R. S. Kumar, and S. A. Sharavan, "A review of quantum communication and information networks with advanced cryptographic applications using machine learning, deep learning techniques," *Franklin Open*, vol. 10, p. 100223, 2025.

[6] C. H. Lee, K. H. Lim, and S. Eswaran, "A comprehensive survey on secure healthcare data processing with homomorphic encryption: attacks and defenses," *Discover Public Health*, vol. 22, no. 1, pp. 1–29, 2025.

[7] M. Liang, "Teleportation-based quantum homomorphic encryption scheme with quasi-compactness and perfect security," *Quantum Information Processing*, vol. 19, no. 1, p. 28, 2020.

[8] ——, "Quantum fully homomorphic encryption scheme based on universal quantum circuit," *Quantum Information Processing*, vol. 14, no. 8, pp. 2749–2759, 2015.

[9] L. Yu, C. A. Pérez-Delgado, and J. F. Fitzsimons, "Limitations on information theoretically secure quantum homomorphic encryption," *arXiv preprint arXiv:1406.2456*, 2014.

[10] A. Broadbent and S. Jeffery, "Quantum homomorphic encryption for circuits of low t-gate complexity," in *Annual Cryptology Conference*. Springer, 2015, pp. 609–629.

[11] S. Ganjian, C. Paddock, and A. Broadbent, "Demonstrating quantum homomorphic encryption through simulation," in *2024 IEEE International Conference on Quantum Computing and Engineering (QCE)*, vol. 2. IEEE, 2024, pp. 593–594.

[12] C. Gong, Z. Dong, A. Gani, and H. Qi, "Quantum ciphertext dimension reduction scheme for homomorphic encrypted data," in *2021 IEEE 20th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*. IEEE, 2021, pp. 903–910.

[13] P. Fernández and M. A. Martin-Delgado, "Homomorphic encryption of the k= 2 bernstein–vazirani algorithm," *Journal of Physics A: Mathematical and Theoretical*, vol. 57, no. 36, p. 365301, 2024.

[14] C. Gong, J. Du, Z. Dong, Z. Guo, A. Gani, L. Zhao, and H. Qi, "Grover algorithm-based quantum homomorphic encryption ciphertext retrieval scheme in quantum cloud computing." *Quantum Information Processing*, vol. 19, no. 3, 2020.

[15] S. A. Ortega, P. Fernández, and M. A. Martin-Delgado, "Implementing semiclassical szegedy walks in classical-quantum circuits for homomorphic encryption," *Journal of Physics: Complexity*, vol. 6, no. 2, p. 025010, 2025.

[16] S. Seyedi and H. Abdoli, "Optimized design of lower complexity reversible toffoli gate in qca technology," in *2024 6th Iranian International Conference on Microelectronics (IICM)*. IEEE, 2024, pp. 1–5.

[17] X. Huang, S. Zhang, Y. Chang, F. Yang, M. Hou, and W. Cheng, "Quantum secure direct communication based on quantum homomorphic encryption," *Modern Physics Letters A*, vol. 36, no. 37, p. 2150263, 2021.

[18] Z.-Z. Li, M.-K. Liu, W.-L. Yang, B. Gao, and Z.-C. Li, "Multi-party dynamic quantum homomorphic encryption scheme based on rotation operators," *arXiv preprint arXiv:2505.06955*, 2025.

[19] G. Ma and H. Li, "Quantum fully homomorphic encryption by integrating pauli one-time pad with quaternions," *Quantum*, vol. 6, p. 866, 2022.

[20] P. Fernández and M. A. Martin-Delgado, "Implementing the grover algorithm in homomorphic encryption schemes," *Physical Review Research*, vol. 6, no. 4, p. 043109, 2024.

[21] G. Biswas, "On classical simulation of quantum circuits composed of clifford gates," *arXiv preprint arXiv:2405.13590*, 2024.

[22] L. Biswal, D. Bhattacharjee, A. Chakrabarti, and A. Chattopadhyay, "Synthesis techniques for fault-tolerant quantum circuit implementation using clifford+ zn-group," *ACM Transactions on Quantum Computing*, vol. 5, no. 3, pp. 1–14, 2024.
[23] F. Butt, S. Heußen, M. Rispler, and M. Müller, "Fault-tolerant code-switching protocols for near-term quantum processors," *PRX Quantum*, vol. 5, no. 2, p. 020345, 2024.
[24] J. Preskill, "Quantum computing in the nisq era and beyond," *Quantum*, vol. 2, p. 79, 2018.
[25] M. AbuGhanem, "Practical fidelity limits of toffoli gates in superconducting quantum processors," *arXiv preprint arXiv:2509.05395*, 2025.
[26] G. Cenedese, G. Benenti, and M. Bondani, "Correcting coherent errors by random operation on actual quantum hardware," *Entropy*, vol. 25, no. 2, p. 324, 2023.
[27] Z. Cai, R. Babbush, S. C. Benjamin, S. Endo, W. J. Huggins, Y. Li, J. R. McClean, and T. E. O'Brien, "Quantum error mitigation," *Reviews of Modern Physics*, vol. 95, no. 4, p. 045005, 2023.
[28] X.-Y. Xu, C. Ding, and W.-S. Bao, "Efficient measurement error mitigation with subsystem-balanced pauli twirling," *arXiv preprint arXiv:2509.17298*, 2025.