Secure Delegated Quantum Approximate Optimization Algorithm with Quantum One-Time Pad for MAX-CUT Problem

Juyoung Kim and Doyoung Chung

***Abstract*—In this paper, we propose a secure framework that integrates the Quantum Approximate Optimization Algorithm (QAOA) with the Quantum One-Time Pad (QOTP) to solve optimization problems—specifically the MAX-CUT problem—within a delegated (cloud-based) quantum computing environment while protecting sensitive data. In the proposed approach, the client prepares the initial quantum state and configures the connectivity of the problem's graph using Hadamard and CNOT gates, subsequently encrypting the state with QOTP using a randomly generated key. The encrypted state is then transmitted to the server, which performs the necessary operations (such as R gate operations) without accessing sensitive information. After the operations, the client decrypts the returned state using the client's secret key and measures the outcome to obtain an approximate solution. This method leverages the advantages of quantum parallelism and optimization while ensuring data confidentiality, offering a novel approach to secure delegated quantum optimization.**

***Index Terms*—Delegated Quantum Computing, Quantum Approximate Optimization Algorithm (QAOA), Quantum One-Time Pad (QOTP)**

I. Introduction

Quantum computing technology matures, quantum processing is being applied to complex algorithms that are challenging for classical computers. Quantum computing leverages phenomena such as superposition and entanglement to achieve exponential speed improvements over classical systems. These characteristics not only maximize computational efficiency via specialized quantum algorithms but also offer inherent advantages for maintaining data confidentiality.

The Quantum Approximate Optimization Algorithm (QAOA) harnesses the computational power of quantum devices to derive approximate solutions. QAOA operates by employing quantum gates and adjusting parameters, while classical optimization techniques iteratively refine these parameters. It converges toward an approximate solution in an iterative manner, with the Max-Cut problem serving as a representative application. In the Max-Cut problem, graph nodes are partitioned into two sets to maximize the number of edges connecting nodes from different sets, addressing issues such as interference between base stations and efficient network segmentation. When applied to the Max-Cut problem, the parallel processing capability provided by quantum superposition enables more efficient approximations.

Thanks to the properties of quantum entanglement and superposition, a qubit's state remains indeterminate until measurement, a feature that is critical for confidentiality. If an attacker observes a qubit during computation or communication, the act of measurement immediately compromises its confidentiality, offering a higher level of security compared to conventional systems. Since the state is unknown until measured, predicting the outcome is extremely difficult. By leveraging these quantum traits, operations can be executed on an encrypted state using the Quantum One-Time Pad (QOTP), which secures the initial state with a secret key. This approach produces an effect similar to homomorphic encryption in classical environments while reducing computational complexity. In this paper, we propose a method that integrates QOTP with QAOA, enabling the derivation of approximate solutions while safeguarding the privacy of the original data. This integration makes it feasible to implement data privacy protection schemes in a quantum computing environment—an achievement that has been challenging in conventional settings. Specifically, by combining QAOA and QOTP, optimization can be performed on the encrypted state of the data, ensuring that sensitive information remains shielded from external exposure.

Integration is carefully designed to preserve the integrity of the original quantum state even after repeated encryption and decryption operations. By maintaining a strict separation between the client and server roles, our framework minimizes the risk of data leakage. The client's responsibility in generating and managing encryption keys is crucial to ensure that the server, which handles most quantum operations, remains unaware of any sensitive information. In addition, QAOA overcomes the limitations of classical algorithms by merging classical optimization with quantum processing, thereby achieving enhanced efficiency through quantum parallelism. This approach applies to a wide range of problems that are difficult to solve using classical methods and holds significant promise for large-scale datasets or complex computations. For instance, in graph optimization problems such as the Max-Cut problem, QAOA demonstrates considerably improved performance compared to traditional algorithms by concurrently exploring multiple states through superposition and entangle-

Juyoung Kim is with the Cryptography Engineering Laboratory, Electronics and Telecommunications Research Institute (ETRI), Daejeon, South Korea. Email: ap424@etri.re.kr.

Doyoung Chung is with the Cryptography Engineering Laboratory, Electronics and Telecommunications Research Institute (ETRI), Daejeon, South Korea. Email: thisisdoyoung@etri.re.kr.

ment, effectively harnessing the unique computational power of quantum computers.

Complementing this, QOTP plays a critical role in maintaining data confidentiality during quantum operations. Unlike classical encryption, quantum encryption strengthens security by dynamically altering the encrypted state upon observation, ensuring that sensitive information remains protected throughout the computation and that any attempt at unauthorized observation is immediately detectable. Consequently, the combination of QAOA and QOTP offers a powerful tool for efficiently solving optimization problems while guaranteeing robust data privacy in a quantum computing environment. The approach proposed in this paper aims to merge the advantages of both techniques to develop a practical method for quantum optimization that maintains data confidentiality, further expanding the potential of data privacy protection technologies within the realm of quantum computing.

II. BACKGROUND

Numerous investigations have sought either to enhance traditional algorithms used in classical computing environments or to develop novel approaches that exploit the distinctive capabilities of quantum computers. For instance, Shor's algorithm [1] has demonstrated a clear quantum advantage in integer factorization, while Grover's algorithm [2] has significantly improved data search efficiency. Beyond these breakthroughs, a wide range of quantum computing–based algorithms have been explored. In particular, the QAOA [3] is designed to tackle combinatorial optimization challenges by approximating solutions through careful optimization of quantum circuit depth and parameter tuning. Consequently, many studies are actively pursuing methods to boost QAOA's performance and enable efficient implementations.

One early approach proposed exploiting the intrinsic symmetry of the objective function within QAOA [4]. This study examined how leveraging the inherent symmetry in combinatorial optimization problems can lead to more efficient quantum circuits. By reducing the required number of quantum gates and minimizing circuit depth, the impact of noise was significantly diminished.

Further research focused on optimizing the ansatz design for QAOA in solving the Max-Cut problem [5]. This work analyzed in detail the influence of the ansatz structure and its parameters on algorithm performance, demonstrating that an optimized ansatz design can markedly improve the accuracy of QAOA's approximate solutions.

An end-to-end protocol was also proposed for the efficient optimization of QAOA parameters using a reduced number of shots [6]. The study confirmed that even with a configuration of five QAOA layers, stable and high-quality parameters could be achieved despite hardware noise.

To further support both research and practical implementations of QAOA, a reproducibility toolkit named QAOAKit was introduced [7]. This tool facilitates the integration, standardization, and cross-validation of established parameters for the Max-Cut problem, proving valuable for reproducing, comparing, and extending results from various studies.

A novel method for evaluating QAOA performance based on the approximation ratio of individual samples has been proposed [8]. Unlike conventional evaluation methods that focus on average outcomes or expected values, this approach provides a more precise assessment by analyzing the approximation ratios of individual samples. Detailed statistical analyses on 3-regular random graphs revealed that QAOA's performance is highly sensitive to the specific characteristics of the graph.

In environments with a limited number of qubits, a hierarchical strategy known as QAOA-in-QAOA (QAOA^2) was proposed to tackle large-scale Max-Cut problems [9]. This nested QAOA structure enables even small-scale quantum computers to handle complex, large-scale optimization tasks, and the study demonstrated that QAOA^2 can outperform classical computing methods when applied to graphs with thousands of nodes.

Comparative studies have also evaluated the performance of QAOA relative to other optimization algorithms, such as quantum annealing and simulated annealing [10]. These studies systematically compared the algorithms across various combinatorial optimization problems, considering factors like optimization accuracy, computational time, and algorithmic complexity. Results indicated that, under optimal conditions—when the problem structure and quantum circuit depth are appropriately tuned—QAOA can surpass both quantum and simulated annealing. However, they also noted that increased circuit depth may lead to performance degradation due to noise and quantum decoherence.

Additional research has focused on optimizing QAOA performance in noisy quantum environments. Specifically, the effects of classical optimizers and ansatz depth on QAOA performance were carefully analyzed [11]. Various classical optimization algorithms were employed to adjust the QAOA parameters, and the resulting performance variations in noisy settings were examined. The study further highlighted that as the ansatz depth increases, circuit complexity and noise susceptibility grow, underscoring the need to determine an optimal ansatz depth.

Furthermore, analyses have indicated that achieving a significant quantum speedup in solving the Max-Cut problem with QAOA may require the use of hundreds of qubits [12]. Systematic evaluations across graphs of different sizes and circuit depths have concluded that small-scale quantum computers do not exhibit a clear speedup over classical algorithms; thus, large-scale quantum systems with several hundred or more qubits are essential to realize a practical quantum advantage.

These developments in quantum algorithms have motivated research into new computational paradigms. One such paradigm is Delegated Quantum Computation (DQC), where a client with limited quantum capabilities outsources a computation to a powerful but potentially untrusted remote quantum server. The primary goal of DQC is to ensure the privacy of the client's input, output, or the entire computation itself. The two main approaches to achieve this are Blind Quantum Computation (BQC), where the server performs operations without learning any information about the computation it is performing, and Quantum Homomorphic Encryption (QHE),

which involves performing computations directly on encrypted quantum data. Our work falls into the latter category, utilizing a specific QHE scheme to secure a delegated QAOA protocol.

Recently, Quantum One-Time Pad and Quantum Homomorphic Encryption have emerged as pivotal research topics in quantum information processing and security. By harnessing the unique physical properties of quantum systems, these technologies enable secure and efficient data processing on encrypted data, thereby enhancing usability while preserving privacy. Consequently, active research in this domain is underway.

Fisher et al. [13] experimentally demonstrated that a client can securely encrypt its quantum data using QOTP and then delegate computations to a remote quantum server operating directly on the encrypted data, yielding the correct final result. This approach maintains data confidentiality during computation by exploiting homomorphic properties that allow quantum algorithms to run on ciphertext without decryption—a crucial step toward secure quantum cloud computing and remote quantum services.

Broadbent et al. [14] introduced the concept of quantum homomorphic encryption, which enables direct computation on encrypted quantum data without prior decryption. Their work specifically addressed the efficient execution of operations such as Clifford gates and the complexity challenges posed by circuits that incorporate non-Clifford T-gates. They proposed two schemes: one where decryption complexity scales quadratically with the number of T-gates, and another that employs an evaluation key of polynomial length when T-gate depth is constant. Both schemes are built upon classical fully homomorphic encryption frameworks and adhere to modern cryptographic security definitions against chosen plaintext attacks.

Building on insights from fully homomorphic encryption, Liang [15] proposed a quantum fully homomorphic encryption scheme tailored for quantum information processing. Based on a universal quantum circuit, this scheme permits arbitrary quantum transformations on encrypted data while theoretically guaranteeing perfect security. Moreover, by managing the decryption key separately from the unrevealed encryption key, the evaluation algorithm functions independently of the encryption key, making the scheme particularly well-suited for delegated quantum computing. Together, these features provide a robust technical foundation for secure quantum cloud computing and reliable quantum information processing systems.

Meanwhile, proposals for quantum homomorphic encryption schemes that integrate quantum error-correcting codes have also attracted attention [16]. In quantum computing, error correction must be performed without measuring the quantum state, which is analogous to homomorphic encryption that computes on encrypted data. This research integrated error correction codes with encryption into a single process, thereby simultaneously enhancing both the security and efficiency of the system.

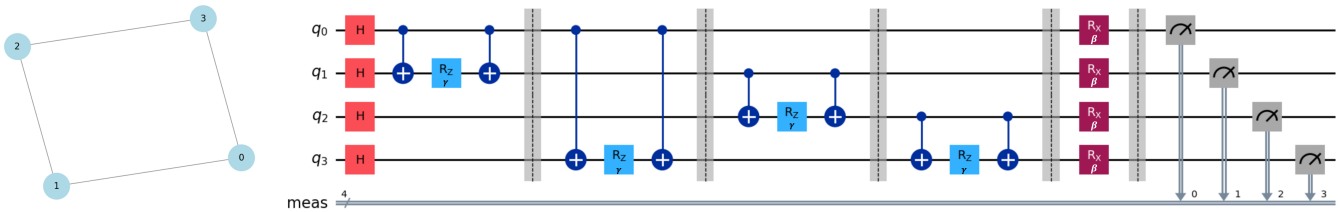
An approach for executing Grover's algorithm—a quantum search algorithm—on encrypted data was also explored [17]. This study demonstrated that when user input data is provided in an encrypted form via quantum homomorphic encryption, a server can execute Grover's algorithm on the encrypted data and return the results, opening up the possibility of securely performing complex quantum operations such as encrypted database searches.

While prior works like Wang et al. [18] and Li et al. [19] establish important foundations for delegated quantum optimization, a practical comparison reveals critical trade-offs in operational responsibility and resource efficiency between the BQC-based model of Wang et al. and our proposed QOTP-based protocol. A core difference lies in who implements the continuous QAOA parameters, γ and β. The BQC protocol of Wang et al. requires the client to perform measurements at arbitrary, continuous angles. While this makes the protocol compatible with QAOA, it places a significant technological burden on the supposedly resource-limited client. Implementing precise measurements at arbitrary angles requires sophisticated analog control, which can be a demanding task. Our proposed protocol resolves this by delegating the burden of performing these precise rotational operations (the R gate) to the powerful, full-fledged quantum server. The client's role is focused on the tasks of setting up the graph structure and encrypting/decrypting the state before and after the main computation, while the critical analog task of implementing the precise angles is offloaded. Furthermore, the protocols differ significantly in qubit efficiency. The BQC model can have a high qubit overhead for setting up the necessary resource state. For example, the Wang et al. paper uses a 10-qubit resource state to implement a simple 2-qubit operation ($H \otimes T$). In contrast, our protocol is much more direct. Our protocol requires only 3 qubits in total (2 problem qubits + 1 ancillary qubit for the non-Clifford T-gate). This superior qubit efficiency is a significant practical advantage in the resource-constrained NISQ era.

Similarly, a comparison with the QHE-based protocol of Li et al. [19] reveals a crucial difference in parameter precision. To handle continuous parameters for general VQAs, their protocol explicitly relies on the Solovay-Kitaev algorithm to decompose the required continuous rotations into a sequence of discrete gates. This process, while enabling universality for a weak client, inevitably introduces a quantization error, which can limit the ultimate precision of the optimization . Our protocol, in contrast, avoids this approximation step by having the server directly execute the rotations with the precise, continuous angles found by the optimizer. This highlights a different trade-off: Li et al. achieve a weaker client (requiring only X, Z gates) at the cost of parameter precision, whereas our work requires a more capable client (requiring $CNOT$ gates) to achieve higher precision by eliminating quantization error.

Our protocol carves out a unique niche in the landscape of secure delegated VQAs. By requiring a client with $CNOT$ gate capability—a higher requirement than in the compared BQC and QHE schemes—it achieves two critical advantages: (1) superior privacy by concealing the problem graph, and (2) higher precision by avoiding the parameter quantization inherent in other universal secure frameworks. This presents a compelling trade-off for applications where data privacy and

This article has been accepted for publication in IEEE Transactions on Emerging Topics in Computing. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TETC.2025.3626768



(a) (b)

Fig. 1. (a) Graph structure illustrating four nodes (0,1,2,3) connected in a square formation. (b) 4-qubit quantum circuit diagram showing the sequential application of an initial Hadamard gate (H), controlled operations (R_z, $CNOT$, etc.), an $R_x(\beta)$ gate, and final measurements on each qubit (q_0–q_3).

solution accuracy are paramount.

To achieve this, our work builds upon quantum homomorphic encryption techniques, particularly those utilizing the Quantum One-Time Pad (QOTP), which are emerging as critical research areas. In this paper, we propose a method to securely and efficiently implement the QAOA algorithm by first transforming it into a structure amenable to this delegated and encrypted computation. Specifically, Section III details this procedure, Section IV presents simulational validations of the proposed technique, and Section VI concludes the paper with our overall findings.

III. Secure Delegated QAOA with QOTP Integration for MAX-CUT Problem

The QAOA is an innovative quantum algorithm that leverages inherent quantum features—such as superposition and entanglement—to search for approximate solutions to combinatorial optimization problems. The algorithm is fundamentally composed of two stages: encoding the problem into a quantum circuit and adjusting the circuit parameters using classical optimization techniques. In the encoding stage, a Hamiltonian corresponding to the optimization problem (e.g., the MAX-CUT problem) is defined and incorporated into the quantum circuit to represent the problem's structure and constraints. In the parameter tuning stage, parameters such as the rotation angles of the circuit's gates are optimized via classical algorithms, guiding the final measurement outcomes toward an optimal or near-optimal solution. In this chapter, based on the basic principles of QAOA, we present an integrated approach that combines a modified QAOA algorithm with the quantum one-time pad (QOTP) technique to perform efficient optimization computations while safeguarding the client's sensitive information in a secure delegated computing environment.

In this integrated approach, the modified QAOA algorithm is executed on a quantum circuit where the problem is encoded using a cost Hamiltonian and a mixer Hamiltonian. The algorithm is run in an environment where quantum one-time pad (QOTP) encryption is applied to the quantum states prior to delegation. This encryption involves applying randomly chosen Pauli operators to the quantum state, thereby masking the state before remote processing. The classical optimization stage then processes the measurement outcomes from the encrypted circuit to determine near-optimal parameter values. Simulations using quantum circuit simulators have shown that this method maintains solution quality comparable to that of conventional QAOA while ensuring that sensitive information is protected. The results confirm that the introduction of QOTP encryption does not compromise the circuit's ability to encode the optimization problem, and that delegated operations can be executed without performance loss.

A. Design of a Modified QAOA for Delegated Computation

In this study, we apply QAOA to derive approximate solutions for the MAX-CUT problem. QAOA proceeds through five sequential steps: state initialization, cost operator implementation, mixer operator application, iterative classical optimization, and final measurement. This sequence is designed to steer the quantum system toward an optimal or near-optimal solution.

Initially, the client applies Hadamard gates to all qubits to generate a uniform superposition state. This is performed by applying the Hadamard operator $H^{\otimes n}$ to the initial state $|0\rangle^{\otimes n}$, resulting in:

$$|\psi\rangle = H^{\otimes n}|0\rangle^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle \tag{1}$$

Next, in the problem encoding phase, the cost Hamiltonian H_C corresponding to the MAX-CUT problem is defined and mapped onto the quantum circuit. To implement the interactions associated with each edge in the graph, $CNOT$ gates are combined with R_z gates. The cost operator is expressed as:

$$U_C(\gamma) = e^{-i\gamma H_C}, \quad H_C = \frac{1}{2}\sum_{(i,j)\in E}(I - Z_iZ_j) \tag{2}$$

where γ is a parameter adjusted dynamically by a classical optimization algorithm.

Subsequently, the mixer operator is applied to facilitate transitions among candidate solutions. This is achieved by applying the mixer Hamiltonian H_M via:

$$U_M(\beta) = e^{-i\beta H_M}, \quad H_M = \sum_{i=1}^{n} X_i \tag{3}$$

Here, β is iteratively updated using classical optimization methods (e.g., Adam, COBYLA).

Following these quantum gate operations, the state of the quantum circuit is measured, producing classical bitstrings

that represent candidate solutions. The quality of a measured bitstring z is evaluated using the cost Hamiltonian H_C, i.e., by computing its classical cost $C(z) = \langle z|H_C|z\rangle$. To systematically explore the parameter space, QAOA employs classical optimization to iteratively update γ and β. Specifically, the parameters are optimized by maximizing the expectation value $\langle H_C\rangle$, estimated from multiple measurement shots. We employ gradient-free methods such as COBYLA, which are effective when the landscape does not readily admit gradient-based techniques. In each iteration, the quantum circuit is executed many times (shots) to obtain a statistical distribution of outcomes; based on these data, the classical optimizer refines the parameters to increase the estimated objective. The iterative quantum–classical loop continues until convergence criteria—such as minimal parameter updates or stabilization of $\langle H_C\rangle$—are satisfied, indicating that the solution is approaching an optimal or near-optimal cut.

After these operations, the rotation angles of the R_x and R_z gates are continuously updated based on the outcomes of multiple quantum measurements, and the circuit gradually converges toward an approximate solution for the MAX-CUT problem.

Furthermore, in a delegated (cloud-based) computation environment, the client pre-configures the connectivity between nodes using $CNOT$ gates and then transmits an encrypted quantum state to the cloud server. The server performs only the R gate operations on this encrypted state, ensuring that the node information remains securely managed via the client's encryption keys. This approach enhances security by preventing the cloud server from accessing sensitive problem data while still enabling efficient quantum computation.

Figure 1(a) shows a simple graph with four nodes arranged in a square. Each node (labeled 0, 1, 2, and 3) is connected to its adjacent nodes. Based on this structure, the MAX-CUT problem is defined to partition the nodes into two sets so as to maximize the number of edges between them.

In the illustrated four-node graph (Fig. 1(a)), each edge is assigned an equal weight of 1, simplifying the cost function for the MAX-CUT problem. The corresponding cost Hamiltonian H_C thus directly penalizes pairs of qubits representing connected nodes when their measurements yield identical values. Explicitly, for an edge connecting nodes i and j, the Hamiltonian term Z_iZ_j has eigenvalues of $+1$ if the states are identical and -1 if they differ, effectively encoding the MAX-CUT objective into the quantum circuit. The explicit form of the Z_i and Z_j operators refers to the standard Pauli-Z matrices acting on qubits i and j, respectively. Similarly, the mixer Hamiltonian H_M, defined as the sum of single-qubit Pauli-X operators, explicitly serves to transition each qubit state between the computational basis states, thus systematically exploring potential solutions. By uniformly assigning weights and clearly defining these operators, the quantum circuit implementation in Fig. 1(b) precisely reflects the original MAX-CUT formulation, facilitating accurate mapping of classical optimization problems to quantum computations.

Figure 1(b) provides an example implementation of the four-node graph using QAOA. In the initialization step, a Hadamard gate is applied to each qubit to create an equal superposition over all possible solutions.

Next, to implement the cost operation corresponding to the Hamiltonian H_C, pairs of qubits corresponding to the graph's edges are subjected to a combination of $CNOT$ and R_z gates, thereby encoding the cost terms for each edge at the circuit level.Subsequently, the mixer operation, corresponding to the Hamiltonian H_M, is applied to each qubit. This involves applying an R_x gate, which facilitates a broader exploration of the solution space and helps the algorithm avoid local optima.

Finally, measurement yields a classical bitstring representing the final state, and based on the measurement outcomes, the rotation angles (e.g., parameters γ and β) are updated via a classical optimization algorithm. Repeating this process allows the QAOA circuit to gradually converge to an approximate solution for the MAX-CUT problem, as visually illustrated in Figure 1(b).

The protocol for the delegated circuit, illustrated in Figure 2, divides the QAOA operations between the client and the server. First, the client prepares the initial state by applying a H gate to each qubit to establish a uniform superposition. Subsequently, the client applies a block of CNOT gates that represents the connectivity of the problem graph. This completes the client's pre-processing tasks. The prepared quantum state is then transmitted to the server, whose role is limited to applying the parameterized rotational gates. Specifically, the server applies the cost-layer gates $R_z(\gamma)$ and the mixer-layer gates $R_x(\beta)$ according to the parameters provided by the client's classical optimization loop. After the server's operations, the state is returned to the client, who performs the post-processing tasks: applying a second, identical block of CNOT gates and performing the final measurements. Our heuristic ansatz, as illustrated in Figure 2, can be viewed as a Trotter-like splitting of the cost and mixer terms rather than an exact Trotter expansion. Therefore the two circuits are not mathematically equivalent and, for generic parameters, yield different measurement distributions. Nevertheless, because the ansatz preserves the cost–mixer structure layer-by-layer, we expect their optimization landscapes to retain similar critical points. In this paper we evaluate the three variants on a 4-node ring (Table 1, Fig. 5, Table 2) and observe that the maximum-cut bitstrings (0101, 1010) dominate across all variants.

B. Delegated QAOA Circuit with QOTP Applied

QOTP encrypts a quantum state by applying Pauli-X and Pauli-Z gates based on a randomly generated classical key [13]. For the initial state $|\psi\rangle$, the client randomly selects a key (a, b) and applies the X^aZ^b operations, transmitting the encrypted state $X^aZ^b|\psi\rangle$ to the server. The server then applies the desired quantum operation U directly on this state, and the client can recover the final outcome $U|\psi\rangle$ by applying the corresponding inverse Pauli operations using the client's secret key. In this process, the quantum state remains encrypted, ensuring that the client's sensitive information is not exposed to the server. Figure 4 illustrates how key values are computed for each gate. Notably, within the QAOA algorithm, operations such as non-Clifford R gates may require additional ancillary qubits.

This article has been accepted for publication in IEEE Transactions on Emerging Topics in Computing. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TETC.2025.3626768

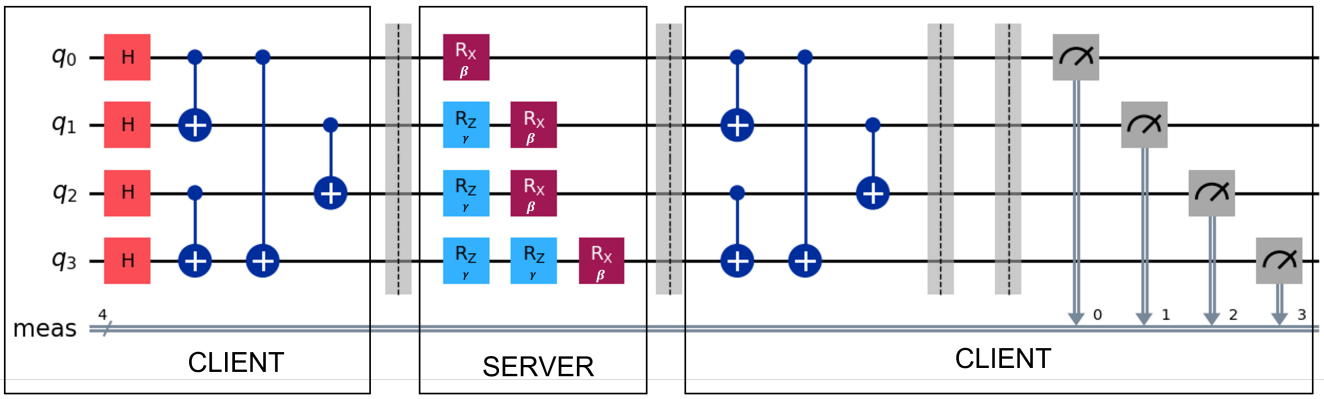


Fig. 2. Proposed 4-qubit modified QAOA circuit for delegated MAX-CUT

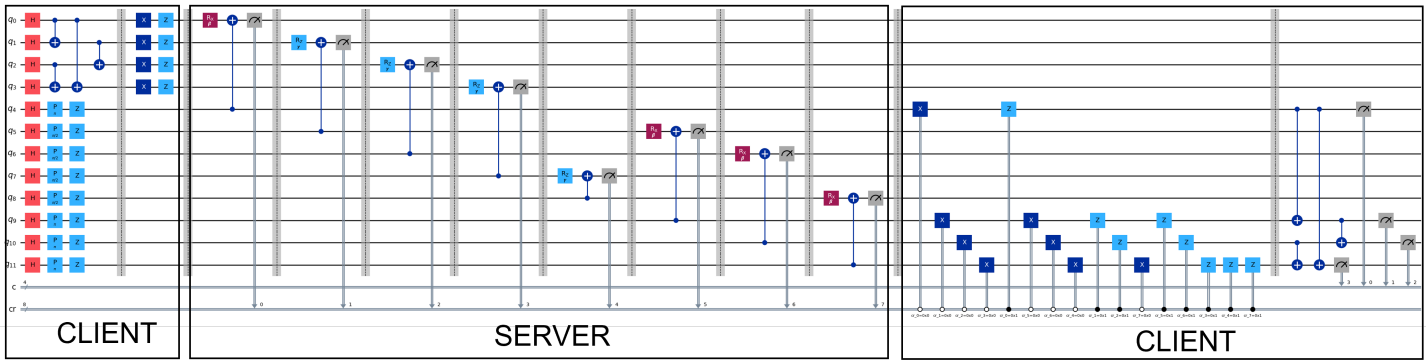


Fig. 3. Quantum circuit for delegated QAOA with QOTP

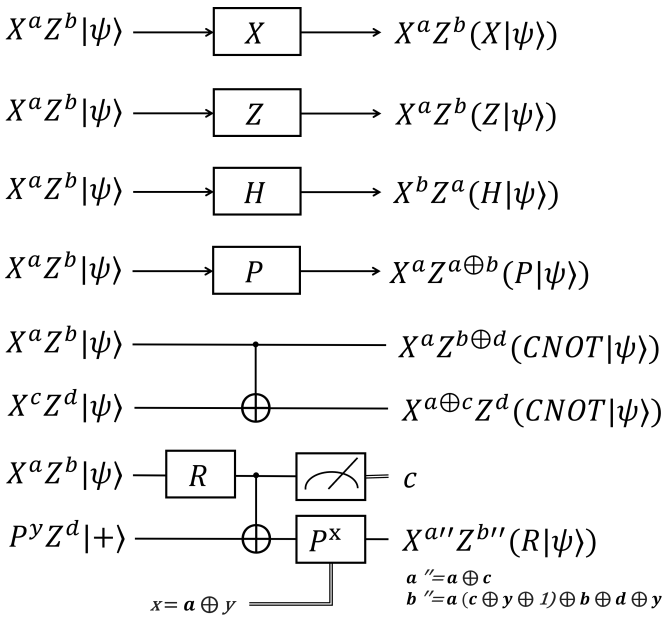


Fig. 4. QOTP key update for universal gates

The proposed quantum circuit in Figure 3 is constructed as follows. The client first applies Hadamard gates to each qubit to form an equal superposition, and then uses $CNOT$ gates to implement the connection structure representing the node connectivity of the problem. Next, by applying X^aZ^b operations to each qubit using the randomly generated key (a, b), QOTP encryption is completed. The keys (a, b) are independently generated per qubit and kept secret by the client. The server does not learn (a, b); when needed, it only receives uniformly random correction bits (classical) that prescribe predetermined Pauli corrections. Consequently, the correction bits observed by the server are information-theoretically independent of (a, b).

The encrypted state is then transmitted to the server, where only the non-Clifford R gate operations required for QAOA are performed. During these R gate operations, ancillary qubits initially prepared in the $|+\rangle$ state are introduced, and corresponding key-dependent corrections are applied as required. After these operations, the state is returned to the client.

Figure 3 visually illustrates the division of responsibilities between the client and server within the proposed delegated QAOA framework. The left section clearly shows the client's initial quantum operations, including state initialization using Hadamard gates, CNOT gate configurations representing graph connectivity, and the subsequent encryption steps. The central server section emphasizes the limited scope of the server's tasks, where it performs only the essential non-Clifford R gate operations and introduces ancillary qubits for key-dependent corrections. Measurements within this section are conditional operations used exclusively for correction and do not yield final computational results. The right section returns control

to the client, who performs the inverse encryption operations and restores the node connectivity. Finally, the client conducts measurements to determine the computational outcomes. This visual depiction highlights the isolation of sensitive quantum state information from the server, underscoring the security-oriented design of the framework. Each operation shown in Figure 3 aligns directly with the theoretical description of client-server interactions and encryption protocols, providing a transparent representation of the secure computation flow.

Upon receiving the state, the client initiates the decryption phase. Using the client's secret key (a, b), the client reverses the $X^a Z^b$ operations to recover the original state or the intended result $U|\psi\rangle$. Simultaneously, the client re-applies the $CNOT$ operations from the initial phase to accurately restore the node connectivity, and final measurements yield an approximate solution to the optimization problem.

The integration of QOTP encryption within the delegated QAOA framework requires synchronization between key management and quantum gate operations. The encryption keys, generated independently for each qubit, are maintained throughout the computation to ensure that operations on the encrypted state yield the correct result upon decryption. In this process, the key-dependent corrections applied during non-Clifford R gate operations and the use of ancillary qubits are coordinated via the standard QOTP key-update rules on the client side; the server applies fixed corrections driven by random bits and learns nothing about (a, b). This coordination ensures that any modifications introduced by the ancillary operations are compensated by the corresponding inverse operations during decryption.

The QOTP protocol theoretically guarantees exact recovery of the final quantum state after decryption, owing to its unitary structure and key-update rules; our numerical simulations merely serve to empirically confirm this proven correctness under simulated noise.

IV. Simulation and Results

In this study, we aimed to solve the Max-Cut problem by implementing three variants of the QAOA:

1) the conventional QAOA algorithm (basic type),
2) a modified QAOA algorithm for delegated operations (proposed type 1),
3) a QAOA algorithm with QOTP applied (proposed type 2).

In this study, we used quantum computing simulators to validate our proposed algorithm. Currently, various forms of quantum computing simulators exist and have been used to obtain extensive results in various fields [20]. To validate the proposed algorithm in simulation, all simulations were conducted using the Qiskit framework and executed on the `Aer qasm_simulator`. The graph in consideration consists of 4 nodes and 4 edges, as illustrated in Figure 1(a). We set the QAOA repetition count p to 1, and for each of the parameters β and γ, we selected 15 evenly spaced values from 0 to π. This produced a total of $15 \times 15 = 225$ parameter combinations. For each combination, the circuit was executed 1024 times (shots) to obtain statistically reliable measurement outcomes.

Since the parameter space is relatively low-dimensional, we adopted a grid search approach rather than a gradient-based optimization method. This allowed us to uniformly explore the entire parameter range, easily run the circuit for each parameter pair, and compare the results. Through this process, we identified the optimal parameter combinations for (1) the conventional QAOA, (2) the modified QAOA for delegated operations, and (3) the QOTP-applied delegated QAOA. We then evaluated the approximation performance of each algorithm by comparing the average cut value against the classical maximum cut value for the given 4-node ring graph.

Figure 5 presents the measurement outcome distributions for the three QAOA variants under their respective optimal parameter settings. In all three histograms, the bitstrings 0101 and 1010 exhibit the highest frequencies, indicating that these solutions yield the maximum cut value in the 4-node ring graph. Specifically, in a cycle of four nodes, assigning alternating nodes (e.g., 0 and 2 in one set, 1 and 3 in the other) ensures that each edge connects nodes in different sets, thereby including all edges in the cut.

A key observation is that the measurement distributions for 0101 and 1010 are similarly prominent across all three algorithms. This result confirms that introducing delegated operations and QOTP does not degrade the optimization performance of QAOA. In particular, the near-identical outcome distributions for proposed types 1 and 2 demonstrate that security-enhancing features can be added without sacrificing the core optimization capabilities of QAOA.

TABLE I
Comparison of QAOA Methods with Parameter Values

No.	Type	β	γ
1	Conventional QAOA	2.019	2.468
2	Delegated QAOA	2.243	2.019
3	Delegated QAOA with QOTP	2.243	1.570

Table 1 compares the optimal parameter values obtained from three QAOA approaches: conventional QAOA, delegated QAOA, and delegated QAOA with QOTP applied.

In QAOA, γ is the rotation angle applied to the cost Hamiltonian, which reflects the cost function of the problem onto the quantum state. In contrast, β is the rotation angle applied to the mixer Hamiltonian, used to effectively expand the search space for solutions.

For conventional QAOA, β is found to be 2.019 and γ is 2.468. This indicates a representative set of parameters for solving the maximum cut problem on a 4-node ring graph using a traditional QAOA circuit configuration. In the delegated QAOA approach, the division of roles between the client and the server alters the circuit's operation order and phase adjustment, resulting in an increase of β to 2.243 and a decrease of γ to 2.019.

For the delegated QAOA with QOTP applied, β remains the same as in the delegated method at 2.243, while γ further decreases to 1.570. This outcome is interpreted as a consequence of the additional random Pauli operations introduced during the QOTP encryption process, which change the phase

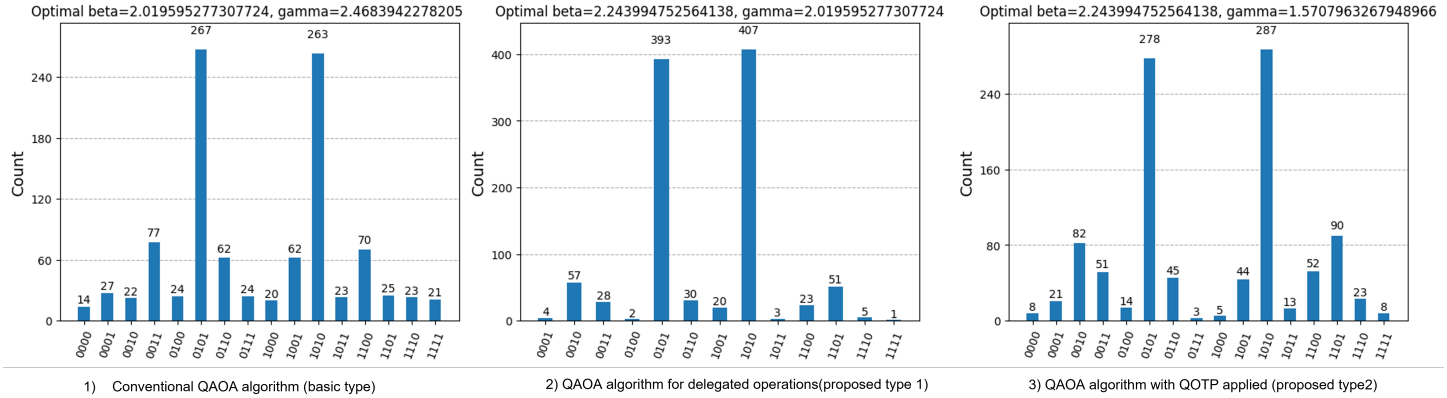


Fig. 5. **Measurement outcome distributions for the three QAOA variants.** Each histogram shows the frequencies of the 16 possible 4-qubit measurement outcomes (bitstrings) observed over 1024 shots at the respective optimal parameter combinations. The left histogram corresponds to the conventional QAOA (basic type), the middle to the delegated QAOA (proposed type 1), and the right to the QOTP-applied delegated QAOA (proposed type 2). The x-axis lists all bitstrings from 0000 to 1111, while the y-axis indicates how many times each bitstring was measured. Notably, the bitstrings 0101 and 1010 appear most frequently across all three variants, matching the maximum cut solutions for the 4-node ring graph.

adjustment in the circuit and result in a lower optimal rotation angle for the cost Hamiltonian.

All three approaches yield β values distributed approximately between 2.0 and 2.243, while γ is highest in conventional QAOA and decreases in the delegated and QOTP-applied methods. These results reflect the impact that differences in circuit configuration and computational mechanisms have on the selection of optimal parameters. In particular, the introduction of QOTP brings about a distinct change in the phase adjustment of the circuit, significantly influencing the optimization of γ.

Table 1 shows that the optimal parameters (β, γ) shift across variants. This is expected, as the classical optimizer explores each circuit's unique optimization landscape. The delegation and encryption layers apply unitary transformations to the circuit, which can alter the landscape's shape and shift the numerical location of its optima. However, the extremal achievable expectation values $\langle H_C \rangle$ are preserved under such transformations. This means the fundamental structure of the landscape, including the value of the MAX-CUT solution, remains intact. As evidenced by Fig.5 and Table 2, all variants exhibit consistent dominance of the correct MAX-CUT bitstrings, and the optimizer finds parameters yielding those solutions. This confirms that QAOA's variational loop operates robustly despite the structural changes of the proposed protocol.

To further examine the influence of these phase adjustments, the probability distributions for optimal parameters were analyzed based on the measurement outcome counts provided in Table 2. For each QAOA variant, measurement outcome distributions were obtained from 1024 shots at the optimal parameters shown in Table 1. Across all methods, the predominant measurement outcomes corresponded to the bitstrings representing the maximum cut solutions, demonstrating consistency despite parameter variations. The similarity in measurement outcomes between the conventional and modified approaches implies that although phase adjustments alter the rotation angles, they do not reduce the probability of

TABLE II
MEASUREMENT OUTCOME COUNTS FOR DIFFERENT QAOA METHODS

Measurement Outcome	Conventional QAOA	Delegated QAOA	Delegated QAOA with QOTP
0000	14	0	8
0001	27	4	21
0010	22	57	82
0011	77	28	51
0100	22	2	14
0101	267	393	278
0110	62	30	45
0111	24	0	3
1000	20	0	5
1001	62	20	44
1010	263	407	287
1011	23	3	13
1100	70	23	52
1101	25	51	90
1110	23	5	23
1111	21	1	8

obtaining optimal solutions. Additionally, the distributions for non-optimal bitstrings showed no significant deviations across the different approaches. This indicates that neither delegated operations nor QOTP encryption introduces systematic bias or instability in the measurement process. Thus, the variations observed in the optimal parameter values reflect adjustments to circuit operations rather than fundamental changes in computational capability or solution reliability. This observation supports the practical applicability of delegated QAOA methods, highlighting that encryption and delegation do not compromise the integrity or performance of the algorithm's quantum computations.

Nevertheless, all three methods successfully produce the maximum cut solutions (0101 and 1010) in the measurement outcomes, confirming that both the delegated QAOA and the QOTP-applied delegated QAOA maintain normal computational performance compared to conventional QAOA.

Therefore, the results suggest that even with additional modifications for delegated computing and data encryption, QAOA retains its strong ability to approximate the maximum cut solution. This finding is significant for practical quantum computing applications, as it indicates that secure, cloud-based quantum optimization can be achieved while preserving the algorithm's intrinsic performance benefits.

V. Security Analysis

The proposed secure delegated QAOA uses QOTP to ensure the confidentiality of sensitive data during quantum computations. In this scheme, an initial quantum state $|\psi\rangle$ is encrypted by applying randomly selected Pauli-X and Pauli-Z operators, as described by

$$|\psi_{\text{enc}}\rangle = X^a Z^b |\psi\rangle, \quad a, b \in \{0,1\}^n \tag{4}$$

where a and b are independent classical random bits for each qubit.

This operation completely randomizes the quantum state, making it statistically indistinguishable from a maximally mixed state for any observer without the secret key. The transformation guarantees the encrypted state is maximally mixed $(I/2^n)$ for any observer without the key, thereby providing information-theoretic security that does not rely on computational hardness assumptions.

However, this security guarantee relies crucially on secure, one-time use of encryption keys. If these keys are compromised or reused, the security would immediately deteriorate. Therefore, robust and secure key management is an essential requirement for practical deployment

The inherent properties of QOTP, its linearity and unitary evolution, ensure that even minimal discrepancies in the key yield uncorrelated results. This robustness is particularly important in the context of delegated quantum computing, where the security of the data must be maintained throughout the entire computational process. The exponential size of the key space further increases the difficulty for any adversary attempting a brute-force attack, since the probability of guessing the correct key is negligibly small.

Previous research provides substantial evidence supporting the security of QOTP. Fisher et al. demonstrated, through an experimental implementation, that quantum data encrypted using QOTP can be securely processed in a delegated quantum computing environment[13]. In their study, the client encrypted the quantum data and transmitted it to a remote server, where quantum operations were performed; subsequent decryption restored the correct output, thus validating the practical security of QOTP. Moreover, theoretical models by Broadbent et al. and Liang have established that irreversible quantum operations can be effectively executed on encrypted data[14][15]. Broadbent et al. proposed a method that enables quantum homomorphic encryption even in circuits with low T-gate complexity, while Liang introduced a fully quantum homomorphic encryption scheme based on universal quantum circuits[14][15]. These studies provide a rigorous foundation for the secure execution of quantum operations on encrypted data.

The integration of QOTP with the QAOA has been extensively evaluated, and empirical studies confirm that the security enhancements do not affect the algorithm's optimization performance. The reason QOTP integration preserves the computational performance of QAOA lies in the linearity and reversibility of quantum operations. The encryption method applies randomized Pauli gates independently to each qubit, which are unitary and thus preserve quantum coherence. Consequently, the state space exploration properties of QAOA remain unaffected by encryption, enabling the algorithm to achieve comparable optimization outcomes. Simulation results indicate that quantum gate sequences for encrypted and unencrypted computations differ primarily in phase adjustments rather than the fundamental structure or computational paths. As long as the correct keys are applied during decryption, any phase alterations introduced by encryption are systematically reversed. Additionally, simulations demonstrate that measurement outcome distributions for encrypted quantum circuits closely align with those from unencrypted circuits, confirming that the optimization quality remains consistent. The fidelity of computational outcomes following encryption and subsequent decryption typically remains near ideal conditions, thereby affirming practical robustness. These characteristics highlight the compatibility of QOTP with quantum optimization techniques, providing evidence of the encryption method's suitability for secure quantum computing tasks.

The encryption process is applied before any quantum operations, and a corresponding decryption step is performed after the operations to recover the original computational output with high fidelity. While the optimal angles differ across variants, the dominant MAX-CUT bitstrings (0101, 1010) remain consistent (Fig. 5, Table 2), indicating that the added security layer does not degrade optimization performance.

Furthermore, the modular nature of QOTP facilitates robust key management. Each qubit is encrypted independently, so overall security is preserved even if a portion of the keys is compromised, provided that a total simultaneous breach does not occur. This characteristic makes QOTP an attractive choice for environments where strict data privacy is essential. In addition, fundamental quantum mechanical principles, such as the no-cloning theorem and the inevitable disturbance caused by measurement, serve as additional safeguards. Any attempt to clone or measure the encrypted state inevitably alters it, alerting the legitimate user to a potential security breach.

The key-dependent corrections for non-Clifford R gates do not leak (a,b). The server only sees uniformly random classical bits derived from encrypted measurement outcomes and applies predetermined Pauli corrections. These bits are information-theoretically independent of the client's secret keys, preventing any key reconstruction attack.

In summary, the integration of QOTP-based encryption with quantum approximate optimization not only achieves superior information-theoretic security but also preserves the algorithm's high computational efficiency.

VI. Conclusion

This paper proposed a method to efficiently solve optimization problems by integrating the Quantum Approximate

Optimization Algorithm with the Quantum One-Time Pad in a secure delegated quantum computing environment. We implemented three variants: standard QAOA, a modified version designed for delegated operations, and a QOTP-enhanced QAOA ensuring improved security. Simulations on a 4-node ring graph demonstrated that all three approaches effectively identified the maximum cut solutions, notably represented by the frequent measurement outcomes of bitstrings 0101 and 1010. These results indicate that adding QOTP-based encryption preserves the intrinsic optimization performance of QAOA.

While our numerical validation was limited to a 4-node ring, the core principles generalize to larger systems. QOTP security scales linearly with qubit count because each qubit is encrypted independently by Pauli operators. Correctness is likewise preserved, as encryption and decryption are unitary; by the standard QOTP key-update rules the Pauli masks can be propagated through the circuit layers, so decrypting after evaluation recovers the same outcome. Practical scalability, however, will ultimately be bounded by hardware noise and classical optimizer overhead; integrating our secure layer into hierarchical methods such as QAOA-in-QAOA is a promising near-term path [9]. However, it is crucial to distinguish the scalability of our security protocol from that of the underlying QAOA algorithm itself. While the QOTP encryption layer does not introduce new scalability bottlenecks, the practical scalability of any QAOA implementation is currently limited by significant challenges. As the number of qubits and circuit depth (p) increase, the computation becomes more susceptible to hardware noise and decoherence, which can degrade performance. Furthermore, the classical optimization of a large number of parameters for large-scale problems becomes a formidable challenge. Therefore, our secure protocol inherits the existing challenges of the QAOA framework. This motivates our discussion on the necessity of integrating our secure layer with advanced error mitigation techniques or hierarchical methods like QAOA-in-QAOA to tackle large-scale problems on near-term devices.

However, the simulations in this study utilized a simple 4-node graph, thus limiting the evaluation of real-world quantum noise and error impacts.

Future research should perform comprehensive experiments on larger-scale graphs using actual quantum hardware to thoroughly assess practical performance implications.

In practical quantum computing scenarios, the presence of noise arising from gate imperfections, decoherence, and measurement errors could significantly affect the performance of QAOA, particularly in more complex or larger-scale problems. Such real-world noise factors may alter the optimization landscape, potentially impacting convergence to optimal solutions and increasing the variance in measurement outcomes. Consequently, future evaluations should include quantitative analyses of the sensitivity of QAOA performance to different types and levels of quantum noise. Performing these studies would clarify the extent to which noise influences the parameter tuning process, the stability of the measured optimal states, and the overall reliability of the algorithm when executed in realistic quantum environments. Additionally, investigating noise-resilient parameter initialization methods or adaptive optimization algorithms designed to accommodate noisy conditions could provide valuable approaches to improve the robustness of QAOA implementations on noisy intermediate-scale quantum (NISQ) devices.

Besides the promising results obtained from the 4-node ring graph simulations, it is important to consider scalability challenges and the potential integration with advanced error mitigation techniques. Future work should explore hybrid models that combine QOTP with quantum error correction schemes to further enhance reliability in noisy environments. Moreover, a detailed analysis of the computational overhead introduced by the encryption process would provide valuable insights into the trade-offs between security and performance—an analysis that is critical for assessing the feasibility of deploying these methods on large-scale quantum systems.

In addition, future studies should emphasize improving key management strategies. Since QOTP security critically depends on the one-time usage and randomness of keys, inadequate key management practices pose significant risks. Integrating robust quantum key distribution schemes may enhance the security and practicality of the proposed method in a realistic quantum computing infrastructure.

Furthermore, integrating robust quantum key distribution protocols with the proposed method could further mitigate key management challenges. A comprehensive study of key lifecycle management, including secure key generation, distribution, and disposal, is essential for ensuring long-term security in delegated quantum computing. Future investigations should also address potential vulnerabilities arising from side-channel attacks and develop countermeasures to protect the encryption keys throughout the computational process.

In summary, this study theoretically and in simulation demonstrates that integrating QOTP with QAOA effectively balances security and optimization performance. Further experimental validation under realistic conditions, quantitative analyses of quantum noise impacts, and advancements in key management techniques will solidify the practicality and reliability of secure delegated quantum optimization schemes.

ACKNOWLEDGMENTS

This work was supported by Electronics and Telecommunications Research Institute(ETRI) grant funded by the Korean government [25ZS1320, Research on Quantum-Based New Cryptographic System for Ensuring Perfect Data Privacy]

REFERENCES

[1] P. W. Shor, "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer," *in Proc. 35th Annu. Symp. Found. Comput. Sci. (FOCS)*, pp. 124-134, 1994.

[2] L. K. Grover, "A fast quantum mechanical algorithm for database search," *in Proc. 28th Annu. ACM Symp. Theory Comput. (STOC)*, pp. 212-219, 1996.

[3] E. Farhi, J. Goldstone, and S. Gutmann, "A Quantum Approximate Optimization Algorithm," *arXiv preprint arXiv:1411.4028*, 2014.

[4] R. Shaydulin, S. Hadfield, T. Hogg, and I. Safro, "Classical symmetries and the Quantum Approximate Optimization Algorithm," *Quantum Information Processing*, vol. 20, no. 11, Kluwer Academic Publishers, USA, Nov. 2021. DOI: 10.1007/s11128-021-03298-4.

[5] R. Majumdar, D. Madan, D. Bhoumik, D. Vinayagamurthy, S. Raghunathan, and S. Sur-Kolay, "Optimizing Ansatz Design in QAOA for Max-cut," *arXiv preprint*, arXiv:2106.02812, 2021. [Online]. Available: https://arxiv.org/abs/2106.02812.

[6] T. Hao, Z. He, R. Shaydulin, J. Larson, and M. Pistoia, "End-to-End Protocol for High-Quality QAOA Parameters with Few Shots," *arXiv preprint*, arXiv:2408.00557, 2024. [Online]. Available: https://arxiv.org/abs/2408.00557.

[7] R. Shaydulin, K. Marwaha, J. Wurtz, and P. C. Lotshaw, "QAOAKit: A Toolkit for Reproducible Study, Application, and Verification of the QAOA," in *Proc. 2021 IEEE/ACM Second Int. Workshop on Quantum Computing Software (QCS)*, 2021, pp. 64–71. DOI: 10.1109/QCS54837.2021.00011.

[8] J. Larkin, M. Jonsson, D. Justice, and G. G. Guerreschi, "Evaluation of QAOA based on the approximation ratio of individual samples," *Quantum Science and Technology*, vol. 7, no. 4, p. 045014, IOP Publishing, Aug. 2022. DOI: 10.1088/2058-9565/ac6973.

[9] Z. Zhou, Y. Du, X. Tian, and D. Tao, "QAOA-in-QAOA: Solving Large-Scale MaxCut Problems on Small Quantum Machines," *Phys. Rev. Appl.*, vol. 19, no. 2, p. 024027, Feb. 2023. DOI: 10.1103/PhysRevApplied.19.024027.

[10] M. Streif and M. Leib, "Comparison of QAOA with Quantum and Simulated Annealing," *arXiv preprint*, arXiv:1901.01903, 2019. [Online]. Available: https://arxiv.org/abs/1901.01903.

[11] A. Pellow-Jarman, S. McFarthing, I. Sinayskiy *et al.*, "The effect of classical optimizers and Ansatz depth on QAOA performance in noisy devices," *Scientific Reports*, vol. 14, p. 16011, 2024. DOI: 10.1038/s41598-024-66625-6.

[12] G. G. Guerreschi and A. Y. Matsuura, "QAOA for Max-Cut requires hundreds of qubits for quantum speed-up," *Scientific Reports*, vol. 9, p. 6903, 2019. DOI: 10.1038/s41598-019-43176-9.

[13] K. Fisher, A. Broadbent, L. Shalm, *et al.*, "Quantum computing on encrypted data," *Nature Communications*, vol. 5, p. 3074, 2014. DOI: 10.1038/ncomms4074.

[14] A. Broadbent and S. Jeffery, "Quantum Homomorphic Encryption for Circuits of Low T-gate Complexity," in R. Gennaro and M. Robshaw (eds.), *Advances in Cryptology – CRYPTO 2015. CRYPTO 2015. Lecture Notes in Computer Science*, vol. 9216. Springer, Berlin, Heidelberg, 2015. DOI: 10.1007/978-3-662-48000-7_30.

[15] M. Liang, "Quantum fully homomorphic encryption scheme based on universal quantum circuit," *Quantum Information Processing*, vol. 14, pp. 2749–2759, 2015. DOI: 10.1007/s11128-015-1034-9.

[16] I. Sohn, B. Kim, K. Bae, W. Song, and W. Lee, "Error-correctable efficient quantum homomorphic encryption using Calderbank–Shor–Steane codes," *Quantum Information Processing*, vol. 24, no. 2, pp. 1–20, Springer, 2025.

[17] P. Fernández and M. A. Martin-Delgado, "Implementing the Grover algorithm in homomorphic encryption schemes," *Phys. Rev. Res.*, vol. 6, no. 4, p. 043109, Nov. 2024. DOI: 10.1103/PhysRevResearch.6.043109.

[18] Y. Wang, J. Quan, and Q. Li, "A Delegated Quantum Approximate Optimization Algorithm," *in Proc. 14th Int. Conf. Wireless Commun. Signal Process. (WCSP)*, Nanjing, China, 2022, pp. 804-808. DOI: 10.1109/WCSP55476.2022.10039146.

[19] Q. Li, J. Quan, J. Shi, S. Zhang, and X. Li, "Secure Delegated Variational Quantum Algorithms," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 43, no. 10, pp. 3129-3142, Oct. 2024. DOI: 10.1109/TCAD.2024.3391690.

[20] KS. Jin , GI. Cha, "QPlayer: Lightweight, scalable, and fast quantum simulator," *ETRI Journal*, vol. 45, no. 2, pp. 304–317, Apr. 2023. DOI: 10.4218/etrij.2021-0442.

Juyoung Kim received M.S. and PhD degrees from Pukyong National University, Busan, South Korea in 2011 and 2019, respectively. He is now working as a senior researcher at Information Security Research Division of Electronics and Telecommunications Research Institute (ETRI). His research interests include open source, secure coding, biometrics, deep learning security, quantum cryptanalysis.

Doyoung Chung received the B.S., M.S., and Ph.D. degrees in the School of Computing from the Korea Advanced Institute of Science and Technology (KAIST). He is currently a senior researcher at the Electronics and Telecommunications Research Institute (ETRI), where he leads a project on Secure Quantum Computing. His main research interests include secure quantum computing, quantum cryptanalysis, and deep learning for cyber security.