2022 13th International Conference on Information, Intelligence, Systems & Applications (IISA) | 978-1-6654-6390-4/22/$31.00 ©2022 IEEE | DOI: 10.1109/IISA56318.2022.9904399

Implementation and Analysis of Quantum Homomorphic Encryption

Maxwell Yarter
SenSIP Center, School of ECEE
Arizona State University
mtyarter@asu.edu

Glen Uehara
SenSIP Center, School of ECEE
Arizona State University
guehara@asu.edu

Andreas Spanias
SenSIP Center, School of ECEE
Arizona State University
spanias@asu.edu

***Abstract*—Growing interest in the field of quantum computing is fueled by quantum computers projected "quantum supremacy" in speed and security. The potential for ultra-high speeds may produce a dramatic change in data science, machine learning, analytics, and information processing. This research study will focus on encryption algorithms where quantum computing may affect protocols and deciphering codes. Specifically, homomorphic encryption (HE) enables mathematical operations to be performed on encrypted data without having to decrypt the data in the process. Quantum homomorphic encryption (QHE) enables quantum circuits to be performed on encrypted qubits. In this research experience for undergraduates (REU) study, we design quantum circuits to implement QHE on a quantum teleportation circuit. The teleportation algorithm is profiled in terms of performance and complexity and comparative results are provided for encoded versus unencoded circuits. This work serves as a building block for encrypting more complex quantum algorithms such as Quantum Neural Networks (QNN).**

***Index Terms*—encryption, quantum computing, qubit, quantum teleportation, cryptography, homomorphic encryption**

I. Introduction

As quantum computing hardware develops its advantages are gradually proven. This development happens in parallel with tools for designing and simulating quantum circuits. These tools allow researchers to design, test, and compare algorithms on quantum computer against classical ones. Executing information processing and machine learning tasks over massive data sets can be incredibly time-consuming depending on the problem. The projected increase in processing speed of quantum computers could revolutionize the field of data science and machine learning. Initial exploration into quantum neural networks (QNNs) has shown promise through their robustness [1], but still need to be improved given current limitations caused by quantum measurement noise.

Quantum computing hardware exists but access is currently limited and generally expensive. Access to quantum simulators, however, is free for university, research, and education purposes. Several companies have developed quantum simulators, including Google [2], IBM [3], Microsoft [4] and Rigetti [5]. The simulators enable researchers to implement their algorithms and assess the performance of quantum machines with regard to quantum noise [6], precision, and quantum circuit complexity.

With the development of multi-stage highly complex information processing algorithms speed, reliability, and data security are of primary importance particularly in the intelligence community [7]. A solution to the problem of data security is encrypting an algorithms parameters so that only certain users with the corresponding encryption key can use it. This process is complicated when the owner of a privileged algorithm wants to lease its use to a third-party. For example, access to a plain-text machine learning algorithm could be used to reverse engineer model parameters and obtain access to original data [8]. Current neural networks also frequently use cloud computing resources to access data which poses additional security risks to the models [9]. Homomorphic encryption is a potential solution to these problems.

Homomorphic encryption was introduced by Rivest, Adleman, and Dertouzos [10] and allows the evaluation of arbitrary functions on encrypted data. In other words, data can be encrypted and passed into an algorithm to obtain an encrypted result. When decrypted the solution will be the same as if you passed in unencrypted data. A flow chart of this process can be seen in Fig. 1. This method secures both a user's data and the parameters of the algorithm they are using. In this study, we will use quantum simulation software to implement a quantum teleportation algorithm with homomorphic encryption.

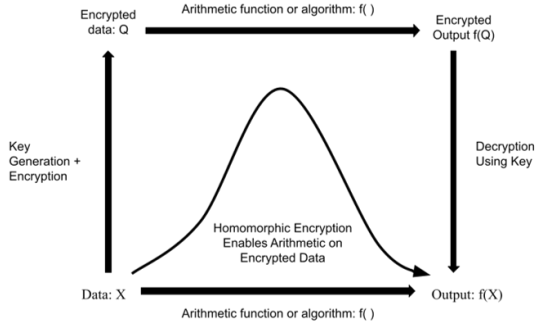


Fig. 1: Conceptual Diagram of Homomorphic Encryption.

Sponsored by SenSIP IUCRC Quantum Machine Learning Project

II. Literature Review

Homomorphic encryption requires special considerations to ensure arithmetic operations preserve encrypted data's integrity. A "noise budget" is imposed by the parameters selected to generate an encryption key. Performing operations on a ciphertext expends this budget and expending it all prevents a solution from being retrieved. In classical computing, an encryption method is considered to be "fully homomorphic" if arbitrarily complex computations can be performed on encrypted data [11]. The first fully homomorphic encryption method was realized in 2009 by Gentry by using ideal lattices [12] and subsequent methods have been designed using other constructs such as the learning with error problem, [13] and the ring learning with error problem [14].

Information processing tasks on classical computers have seen success in the development of homomorphic encryption methods. Li et al. [15] propose an encryption method based on non-albian rings and apply it to multiple machine learning models including logistic regression and Naive Bayes [16]. Bellafqira et al. [17] introduce an encryption method for a secure multilayer perceptron based on the composite residuosity class problem cryptosystem designed by Paillier [18]. Graepel et al. [19] introduce a method that they call *ML Confidential* for machine learning homomorphism.

Quantum mechanics has permanently altered the field of cryptography because it enables new algorithms that were previously impossible. For example, Shors algorithm [20] uses quantum properties to make the integer factoring problem [21] tractable using of qubits. This realization made every public key cryptosystem and all the data encrypted with this protocol vulnerable to attack by powerful quantum computers. Another example of change introduced by quantum properties is quantum key distribution (QKD) [22]. In this case, an eavesdropper can always be detected when creating and distributing encryption keys by using the no-cloning theorem. The security risk posed by quantum encryption-breaking methods is of great interest to defense and commercial entities and has motivated the creating of post-quantum encryption techniques [23].

Naturally, investigation into homomorphic encryption for quantum computers is underway [24]–[26]. Quantum homomorphic encryption requires special considerations to function on qubit operations and quantum circuits. Quantum technology inherently amplifies the noise concerns of encryption. At this time, there is no fully homomorphic encryption method that can execute arbitrary quantum circuits on encrypted data [24]. Despite this, there are existing methods that allow for a limited application of this form of encryption. Tan et al. [25] have developed a quantum homomorphic encryption method that enables a bounding on the information accessible to an unauthorized observer. Additionally, there is a proven homomorphic encryption method for circuits of low T-gate Complexity proposed by Broadbent and Jeffery [26]. This method uses a quantum one-time pad [27] as the basis for encryption over Clifford group circuits and makes the method fully homomorphic by adding a method to encrypt T-gates.

Quantum teleportation is an algorithm that reproduces a prepared qubit state by using an entangled qubit [28]. This allows for the "teleportation" of information stored by a qubit with two classical bits measured from the transmitters system. Generally, this problem is posed as a transmitter named "Alice" who prepares a qubit and wishes to share it with a recipient named "Bob". In a practical setting, this teleportation could be used to transmit qubit states within quantum processing units [29], or across vast distances. Teleportation across a large distance could be enabled through a 3rd party provider that facilitates the qubit entanglement for Alice and Bob. Introducing this third party also introduces the possibility that the system be hijacked, and the qubit state received by the 3rd party provider instead of Bob. QHE is a somewhat trivial solution to this scenario as Alice could keep her two preparation qubits to herself and transmit the classical bits measured from them through a secure channel. If the provider does have access to these qubits, QHE could prevent the interception of sensitive information by encryption prior to handing off the qubits. Without knowledge of the encryption key the classical bit measurements would be corrupted and an incorrect qubit state would be teleported.

III. Proposed Solution

This project attempts to implement the Broadbent et al. [26] encryption method for quantum homomorphic encryption over Clifford group quantum circuits. This set of circuits allows for the implementation of an encrypted qubit teleportation algorithm which will be performed to observe how encryption impacts quantum circuit depth, and coherence. Quantum circuit depth is the length of the longest path of quantum gates in a circuit. Coherence refers to the stability of information held by each qubit and decoherence occurs when noise in a quantum circuit distorts a qubits state destroying the information held therein. The quantum teleportation algorithm was selected because it satisfied two requirements. Firstly, the quantum teleportation consists of Hadamard, X, Z, and CNOT gates [29] which are all stabilizer circuit elements. According to the Gottesman-Knill theorem, [30] stabilizer circuit elements can be simulated efficiently on transistor-based computers. While possible to efficiently simulate a quantum teleportation algorithm on transistor-based computers, real world applications of the algorithm require the use of qubits.

Qiskit was used to implement the Broadbent et al. encryption method for Clifford group circuits. To achieve this goal four steps must be accomplished. These steps are key generation, encryption, quantum circuit application, and decryption. First, to encrypt the qubits two binary strings were randomly generated with length 'n' equivalent to the number of qubits in the operation. These strings served as a simple quantum one-time pad encryption key.

$$[a_0, a_1, ..., a_n], [b_0, b_1, ..., b_n] \tag{1}$$

Encryption over Clifford group circuits is achieved by applying a Pauli gate Q as a one-time pad to any wire

in a quantum circuit. Any set of Clifford gates C that are subsequently applied to the circuit produce an encrypted result to the algorithm. Decryption can then be achieved by applying the conjugate Pauli gate Q'. This relationship between Clifford and Pauli gates can be seen in equation 2.

$$CQ = Q'C \tag{2}$$

The bits in string A correspond to an X gate applied to the associated qubit 'i' and the bits in string B correspond similarly to a Z gate. The application of a random set of X and Z gates to each qubit serves as a quantum one-time pad for encryption of the input data.

$$Q = X^{a_1}Y^{b_1} \otimes ... \otimes X^{a_n}Y^{b_n} \tag{3}$$

From here, homomorphic encryption is achieved by updating the keys after the application of each quantum gate based on a set of update rules [26]. Two key update rules were required to apply the quantum teleportation, an update for the CNOT gate, and an update for the Hadamard gate. The CNOT gate update rule requires updates for bit 'i' associated with the control wire, and bit 'j' associated with the target wire. Bit i of key A is unchanged while bit i of key B is XOR'ed with the bit j of key B. A similar update is applied to bit j of key A. Equation 4 details the update for the control wire and equation 5 details the target wire.

$$f_{a,i} \leftarrow f_{a,i}, f_{b,i} \leftarrow f_{b,i} \otimes f_{b,j} \tag{4}$$

$$f_{a,j} \leftarrow f_{a,i} \otimes f_{a,j}, f_{b,j} \leftarrow f_{b,j} \tag{5}$$

The Hadamard gate requires swapping bits between key A and B for qubit 'i' that the gate is applied to.

$$f_{a,i} \leftarrow f_{b,i}, f_{b,i} \leftarrow f_{a,i} \tag{6}$$

Fig. 2 shows an example quantum circuit of the one-time pad encryption and decryption. The circuit shows two randomly initialized qubits followed by a single CNOT gate with qubit 0 as the control and qubit 1 as the target. Equation 7 shows the original key and the updated key after performing the CNOT gate.

$$[1,0],[1,1] \rightarrow [1,1],[0,1] \tag{7}$$

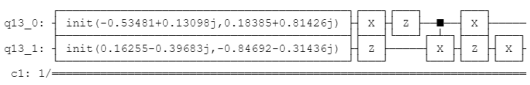


Fig. 2: One-Time Pad and Key Update Rule Applied to CNOT Gate.

IV. Results

The first step to a functional QHE method was creating a quantum one-time pad. This was accomplished through Qiskit by creating an encryption key to apply random X and Z gates to each qubit in a quantum circuit. Two random binary strings of length 'n' equivalent to the number of qubits in the quantum circuit are generated. The associated X and Z gates are then applied based on the binary string's composition.

Encryption was tested on a 3-qubit quantum teleportation circuit where qubits 0 is used as a source and qubit 2 is the destination. Fig. 3 shows the full quantum teleportation circuit. Qubit 0 is initially prepared in the —0¿ state then randomly rotated along the Y and Z axis. After teleportation this rotation is undone by rotating qubit in the opposite directions so that it returns to the —0¿ state. A successful teleportation will then result in a measured bit 0 every time. Fig. 4 applies the one-time pad to the circuit without decrypting the result while Fig. 5 shows the encryption and decryption of the circuit after updating the keys based on the gates used.

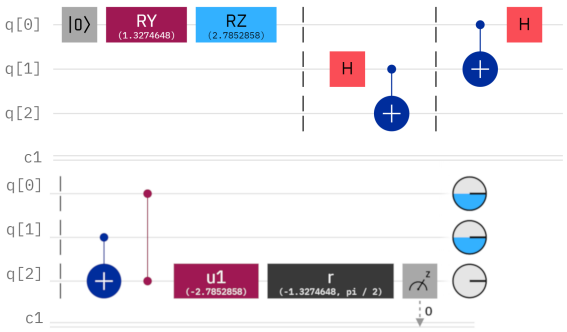


Fig. 3: A 3-Qubit Quantum Teleportation Circuit.

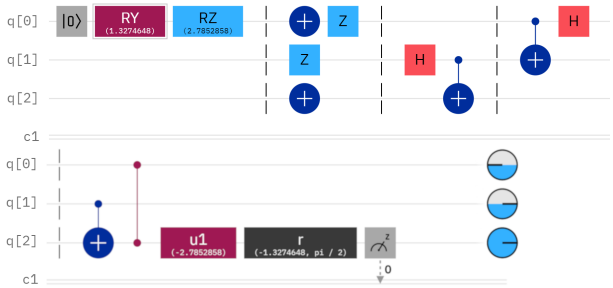


Fig. 4: A 3-Qubit Encrypted Quantum Teleportation Circuit.

After designing each circuit, they were simulated using Qiskit's "qasm" simulator. Each circuit was simulated over 1024 shots and counts for each circuit were plotted in histograms. Quantum teleportation of the qubit state initialized on qubit 0 to qubit 2 is successful if the measured result is a 0. As seen in Fig. 8a and 8c there was a 100 percent success rate of the circuit when it was applied without encryption, and with

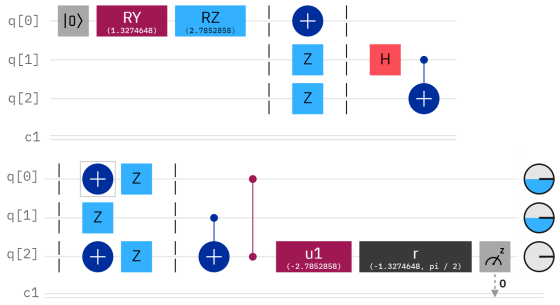


Fig. 5: A 3-Qubit QHE Quantum Teleportation Circuit.

QHE. When the circuit was encrypted but never decrypted as in Fig. 4 the teleportation was unsuccessful as the qubit state received by qubit 2 was different from the original random state. This can be seen as a 4 percent simulation accuracy in Fig. 8b.

For an n qubit system consisting of M stabilizer circuit elements with quantum depth D the cost of homomorphic encryption is minimal. The number of quantum gates in a circuit range from the trivial unencrypted M gates to a maximum of M + 4n total gates. The worst-case scaling is linear with the number of qubits needed for the algorithm. The maximum requires an X and Z gate to encrypt and decrypt each qubit. Quantum circuit depth ranges from the original circuit depth D to D + 4. The maximum impact on depth occurs only in the case where a single qubit is both encrypted and decrypted with X and Z gates. This increase in circuit depth had no impact on the coherence of the quantum teleportation circuit but could cause problems with coherence for circuits with greater depth. Particularly, circuits that approach the threshold for decoherence may become unstable when encrypted. Extending this encryption method to include T gates increases the required gates by more than 4n and requires auxiliary qubits to decrypt operations. [26]

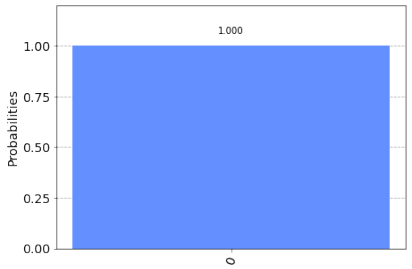
TABLE I: Quantum Teleportation Accuracy Over 1024 Counts.

	Simulation Accuracy (%)
Unencrypted	100
Encrypted	4.39
QHE	100

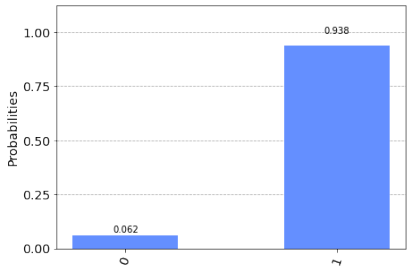
There was no cost to conduct these experiments due to the availability of Qiskit and the qasm simulator backend. Simulations were designed and conducted using a commercial laptop with an Intel core i7 processor.

V. Conclusion

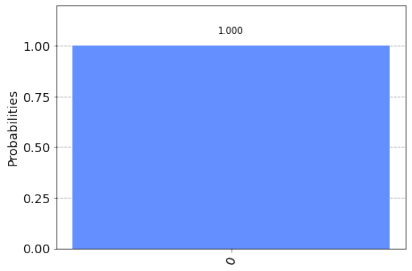
Our SenSIP labs have conducted several quantum computing studies during the last year including quantum machine learning for audio [31] and energy applications [32], [33]. In fact, there are several parallel research and training studies



(a) *Unencrypted*



(b) *Encrypted*



(c) *QHE*

Fig. 6: Simulation Counts for Each Quantum Circuit.

in quantum machine learning [34] design that have been conducted. Other quantum computing education studies have been reported in [35], [36].

In this REU study, we successfully implemented quantum homomorphic encryption over quantum stabilizer circuits. This enables the secure computation of these circuits with little impact on quantum circuit depth relative to the unencrypted circuits. Although rudimentary, compared to classical homomorphic encryption, this is a first step towards providing security for quantum algorithms. Future work should seek to implement full quantum homomorphic encryption by including a protocol for T-gate circuits. Extending the set of circuits that can be encrypted would enable the encryption of quantum information processing algorithms such as quantum neural networks. Secure computation over these quantum algorithms would provide protection to complex quantum algorithms and the large data sets that they could harness.

Acknowledgment

This study was supported in part by the NSF IRES award 1854273, the SenSIP center, and the NSF award 1540040

REFERENCES

[1] G. S. Uehara, A. Spanias, and W. Clark, "Quantum information processing algorithms with emphasis on machine learning," in *2021 12th International Conference on Information, Intelligence, Systems Applications (IISA)*, pp. 1–11, IEEE, jul 2021.

[2] Q. A. team and collaborators, "qsim," Sept. 2020.

[3] S. A. et al., "Qiskit: An open-source framework for quantum computing," 2021.

[4] J. Hooyberghs, *Azure Quantum*, pp. 307–339. Berkeley, CA: Apress, 2022.

[5] R. S. Smith, M. J. Curtis, and W. J. Zeng, "A practical quantum instruction set architecture," 2017.

[6] A. A. Clerk, M. H. Devoret, S. M. Girvin, F. Marquardt, and R. J. Schoelkopf, "Introduction to quantum noise, measurement, and amplification," *Reviews of Modern Physics*, vol. 82, no. 2, p. 1155, 2010.

[7] A. Palfy, "Bridging the gap between collection and analysis: Intelligence information processing and data governance," *International Journal of Intelligence and CounterIntelligence*, vol. 28, no. 2, pp. 365–376, 2015.

[8] A. Dalvi, A. Jain, S. Moradiya, R. Nirmal, J. Sanghavi, and I. Siddavatam, "Securing neural networks using homomorphic encryption," in *2021 International Conference on Intelligent Technologies (CONIT)*, pp. 1–7, 2021.

[9] Y. Aono, T. Hayashi, L. Wang, S. Moriai, *et al.*, "Privacy-preserving deep learning via additively homomorphic encryption," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 5, pp. 1333–1345, 2017.

[10] R. L. Rivest, L. Adleman, M. L. Dertouzos, *et al.*, "On data banks and privacy homomorphisms," *Foundations of secure computation*, vol. 4, no. 11, pp. 169–180, 1978.

[11] V. Vaikuntanathan, "Computing blindfolded: New developments in fully homomorphic encryption," in *2011 IEEE 52nd Annual Symposium on Foundations of Computer Science*, pp. 5–16, 2011.

[12] C. Gentry, "Fully homomorphic encryption using ideal lattices," in *Proceedings of the Forty-First Annual ACM Symposium on Theory of Computing*, STOC '09, (New York, NY, USA), p. 169–178, Association for Computing Machinery, 2009.

[13] Z. Brakerski and V. Vaikuntanathan, "Fully homomorphic encryption from ring-lwe and security for key dependent messages," in *Annual cryptology conference*, pp. 505–524, Springer, 2011.

[14] J. Fan and F. Vercauteren, "Somewhat practical fully homomorphic encryption.," *IACR Cryptol. ePrint Arch.*, vol. 2012, p. 144, 2012.

[15] J. Li, X. Kuang, S. Lin, X. Ma, and Y. Tang, "Privacy preservation for machine learning training and classification based on homomorphic encryption schemes," *Information Sciences*, vol. 526, pp. 166–179, 2020.

[16] M. Malu, G. Dasarathy, and A. Spanias, "Bayesian optimization in high-dimensional spaces: A brief survey," in *2021 12th International Conference on Information, Intelligence, Systems & Applications (IISA)*, pp. 1–8, IEEE, 2021.

[17] R. Bellafqira, G. Coatrieux, E. Genin, and M. Cozic, "Secure multilayer perceptron based on homomorphic encryption," in *International Workshop on Digital Watermarking*, pp. 322–336, Springer, 2018.

[18] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in *International conference on the theory and applications of cryptographic techniques*, pp. 223–238, Springer, 1999.

[19] T. Graepel, K. Lauter, and M. Naehrig, "Ml confidential: Machine learning on encrypted data," in *International Conference on Information Security and Cryptology*, pp. 1–21, Springer, 2012.

[20] M. Hayward, "Quantum computing and shor's algorithm," 2 2005.

[21] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978.

[22] P. W. Shor and J. Preskill, "Simple proof of security of the bb84 quantum key distribution protocol," *Physical review letters*, vol. 85, no. 2, p. 441, 2000.

[23] D. J. Bernstein, "Introduction to post-quantum cryptography," in *Post-quantum cryptography*, pp. 1–14, Springer, 2009.

[24] P. P. Rohde, J. F. Fitzsimons, and A. Gilchrist, "Quantum walks with encrypted data," *Physical Review Letters*, vol. 109, Oct 2012.

[25] S.-H. Tan, J. A. Kettlewell, Y. Ouyang, L. Chen, and J. F. Fitzsimons, "A quantum approach to homomorphic encryption," *Scientific reports*, vol. 6, no. 1, pp. 1–8, 2016.

[26] A. Broadbent and S. Jeffery, "Quantum homomorphic encryption for circuits of low t-gate complexity," *Advances in Cryptology – CRYPTO 2015*, p. 609–629, 2015.

[27] A. Ambainis, M. Mosca, A. Tapp, and R. De Wolf, "Private quantum channels," in *Proceedings 41st Annual Symposium on Foundations of Computer Science*, pp. 547–553, IEEE, 2000.

[28] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, "Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels," *Physical review letters*, vol. 70, no. 13, p. 1895, 1993.

[29] G. Brassard, S. L. Braunstein, and R. Cleve, "Teleportation as a quantum computation," *Physica D: Nonlinear Phenomena*, vol. 120, pp. 43–47, sep 1998.

[30] S. Aaronson and D. Gottesman, "Improved simulation of stabilizer circuits," *Physical Review A*, vol. 70, nov 2004.

[31] M. Esposito, G. Uehara, and A. Spanias, "Quantum machine learning for audio classification with applications to healthcare," *2022 IEEE 13th IISA*, July 2022.

[32] G. Uehara, V. Narayanaswamy, C. Tepedelenlioglu, and A. Spanias, "Quantum machine learning for photovoltaic topology optimization," *2022 IEEE 13th IISA*, July 2022.

[33] G. Uehara, S. Rao, M. Dobson, C. Tepedelenlioglu, and A. Spanias, "Quantum neural network parameter estimation for photovoltaic fault," Proc. IEEE IISA 2021, July 2021.

[34] G. Uehara, J. Larson, A. Spanias, and et al., "Undergraduate research and education in quantum machine learning," IEEE FIE October 2022.

[35] Ö. Salehi, Z. Seskir, and İ. Tepe, "A computer science-oriented approach to introduce quantum computing to a new audience," *IEEE Transactions on Education*, vol. 65, no. 1, pp. 1–8, 2022.

[36] D. Carberry, A. Nourbakhsh, J. Karon, M. N. Jones, M. Jadidi, K. Shahriari, C. Beenfeldt, M. P. Andersson, and S. S. Mansouri, "Building knowledge capacity for quantum computing in engineering education," in *Computer Aided Chemical Engineering*, vol. 50, pp. 2065–2070, Elsevier, 2021.