# All Your Base Are Belong To Us: Stealing VRP Secrets from Quantum Circuit Structures

Jessie Chen
*Yale University*
zixin.chen@yale.edu

Jakub Szefer
*Yale University*
jakub.szefer@yale.edu

***Abstract*—The security and confidentiality of sensitive information processed by quantum computers are of paramount concerns, especially given quantum computers' potential to efficiently solve classically-hard optimization problems. At the heart of many transport optimization tasks lies the Vehicle Routing Problem (VRP), a complex combinatorial optimization issue classified as NP-hard. However, a promising avenue for approximating solutions to VRP is found in the Quantum Approximate Optimization Algorithm (QAOA). This paper demonstrates that analyzing the QAOA quantum circuit structure enables inference of the problem being solved, such as the location or connection of military bases in routing optimization scenarios. By exploiting information leakage, say from side channels, during the QAOA execution, attackers can potentially breach security and retrieve sensitive VRP details, posing profound implications for civilian and national security. This study underscores the need to address and mitigate side-channel vulnerabilities in quantum computing systems to safeguard sensitive information.**

## I. Introduction

Quantum computers promise to deliver exponential speedups over their classical counterparts for certain classes of computational problems. Among the most notable examples are eigenvalue and optimization problems, which have key applications in finance, machine learning, and simulations of quantum chemistry [5], [13], [19]. Moreover, certain NP-hard combinatorial problems like the Vehicle Routing Problem (VRP) can be encoded into Ising Hamiltonians, allowing for solutions via eigenvalue optimization [2], [7]. VRP generalizes the well-known Travelling Salesman Problem (TSP) as there can be multiple vehicles. This makes VRP a popular candidate for optimizing logistics both in civilian and military transportation. Therefore, if one can deduce properties of the problem solved by the VRP, then the confidentiality logistics both in civilian and military transportation could be compromised. Our work aims to elucidate the extent to which this confidentiality may be compromised in the context of quantum computers.

Most current physical quantum computers are so-called Noisy Intermediate-Scale Quantum (NISQ) devices which operate with fewer than 100 qubits and shallow quantum circuit depths [3, 15]. Despite these hardware limitations, the advent of NISQ-era quantum computing has spurred research into short-depth quantum circuits and hybrid quantum-classical algorithms that make use of quantum computers in conjunction with classical optimization techniques. Such hybrid quantum-classical algorithms allow for the possibility of performing useful computational tasks, even with NISQ devices. A crucial milestone in this direction was the invention of the Quantum Approximate Optimization Algorithm (QAOA), proposed by Farhi et al. [6], as a general quantum algorithm that provides approximate solutions for combinatorial optimization problems, including VRPs.

While QAOA efficiently approximates VRPs, its deployment introduces novel security threats, especially those exploiting quantum circuit structures. Previously, various attacks leveraging quantum-specific features, such as reset attacks, fingerprinting tomography, and side-channel attacks, have been identified, raising concerns about information leakage in quantum computing systems, e.g., [4], [12].

In this research, we investigate how security threats from quantum circuit structures can compromise VRPs optimized on quantum computers using QAOA. The routing problem is represented as a graph, such as that of an army base or an airport. The edges can represent transportation capacity of among different bases or airports. The graph being used in VRP is typically a subgraph of some larger, so-called mother graph. For example, the army bases or airports used in a mission are a subset of all the army bases or airports.

In this work we focus on how given a knowledge of the mother graph, and some side channel information from the execution of the QAOA, an attacker can recover the subgraph used in VRP, evaluating their performance across varied graph sizes and noise models pertaining to the side channel information. Our analysis identifies critical security vulnerabilities, emphasizing the importance of preventing attackers from obtaining rotational angles parametrizing gates in quantum circuits. As VRP optimization directly impacts civilian lives and military security, our work addresses crucial security concerns in the quantum computing landscape.

## II. Background

### A. VRP Instance Representation

In this paper, we will represent a problem instance of VRP using $(n, k)$, where $n$ is the number of locations and $k$ is the number of vehicles. For simplicity, we consider the existence of a single depot $D$. We impose two minimum constraints: each location is visited exactly once, and all vehicles begin from and return to the depot $D$. Here $D$ can represent

‡This work was supported in part by NSF grants 2312754 and 2245344; the title borrows the phrase "All Your Base Are Belong To Us" from an old internet meme and the video game Zero Wing [21].

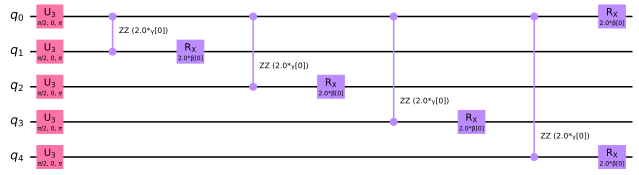

Fig. 1: The circuit representation of a sample variational ansatz for QAOA with $p = 1$. In the circuit, five qubits are used; two-qubit gates consist of RZZ rotational gates and single-qubit gates consist of Rx rotational gates.

mission headquarters, and the locations are the army bases or airports. The vehicles can be airplanes delivering mission-cortical cargo.

### B. Quantum Approximate Optimization Algorithm

The advent of quantum computing has ushered in Quantum Approximate Optimization Algorithm as a quantum solution to VRPs. QAOA, introduced by Farhi et al. [6], offers optimal or near-optimal solutions for various combinatorial optimization problems, including VRPs [10], [23]. Employing variational ansatzes, QAOA encodes the combinatorial problem into a cost Hamiltonian $H_c$ and a heuristic mixer Hamiltonian $H_m$, which is chosen as $H_m = -\sum_i \sigma_i^x$ by convention. Here $\sigma^x$ ($\sigma^z$) is the Pauli X (Z) operator. Generally, a complete variational ansatz for a VRP instance of $(n, k)$ takes the form:

$$\left|\vec{\beta}, \vec{\gamma}\right\rangle = \prod_{i \leq p} e^{-iH_m \beta_i} e^{-iH_c \gamma_i} \left|+\right\rangle^{\otimes n(n-1)}, \tag{1}$$

where $p$ represents the total optimization layers of the quantum circuit, and $\beta_i$, $\gamma_i$ are variational parameters for the layer $i$. They act as overall scaling factors for all the rotational angles in $H_c, H_m$ in the layer $i$. A circuit representation of a sample variational ansatz with $p = 1$ is given in Fig. 1.

The optimization task revolves around minimizing the eigenvalue for $H_c$. Despite its intricacy, studies demonstrate QAOA's ability to acquire quasi-optimal solutions in $O(\text{poly}(p))$ time [23], with adaptive variants showcasing performance improvements [9], [20], [24]. These advancements underscore QAOA's potential in efficiently solving real-world optimization problems, positioning it as a frontrunner for achieving quantum advantage in practical applications.

### C. Constructing VRPs

This paper examines VRPs using real-world datasets sourced from Kaggle, specifically the "USA Airport Dataset" [8], encompassing over 3.5 million domestic flights within the United States from 1990 to 2009. This dataset is a direct extraction from the OpenFlights website and includes detailed information such as the origin and destination airports, passenger counts, flight distances, and dates for each recorded flight.

Focusing on data from 2000 to 2009 and using John F. Kennedy International Airport (JFK) as the depot, we identify airports with nontrivial communication patterns with JFK over the course of nine years and add them as locations in the VRP. Edge weights between airports are determined based on flight distances, passenger counts, and total days elapsed. The resulting VRP graphs are undirected, and edge weights are computed modulo $2\pi$ due to their role as rotational angles in quantum circuit gates.

## III. Threat Model

In this paper, we address the threat posed by an attacker who possesses sufficient knowledge of a mother graph $G$ and targets victims optimizing a VRP defined on some subgraph $G_s \subseteq G$. Assuming ample computing resources, the attacker can precompute all relevant parameters for all $G_s$ subgraphs. Leveraging information extractable from the variational quantum circuits and precomputed parameters, the attacker aims to deduce the specific $G_s$ being optimized.

Under our assumption, the attacker is provided information on the qubit count, gates executed in the quantum circuit and the rotational angles associated with each gate. Although no published techniques exist to achieve this level of granularity, ongoing research endeavors are exploring the utilization of quantum side-channels and crosstalks to achieve similar objectives [4]. Assessing this security threat is prudent and useful given the sensitive nature of the problem.

To alleviate the requirement of acquiring precise rotational angles and incorporate both classical and quantum noise, we introduce imperfect resolution in the rotational angles obtained by the attacker. This imperfect resolution translates into errors and uncertainties in entries of the adjacency matrices representing the VRP graph. We explore various noise distributions within a defined imperfect resolution, including uniform, bimodal, and Gaussian distributions. These distributions will be detailed in subsequent sections.

## IV. Attacker Routine

### A. Cost Hamiltonian and Weight Function

Following the convention used in [2], the quantum cost Hamiltonian for a VRP can be encoded as

$$H_c = -\sum_{i,j<i} J_{ij} \sigma_i^z \sigma_j^z + \sum_i h_i \sigma_i^z + d, \tag{2}$$

where the parameters $J_{ij}, h_i, d$ are determined uniquely from each VRP. In the quantum circuit, the parameter $d$ is proportional to an identity gate and drops out. The parameter of interest to us is $h_i$, which contains the weight for each edge in the VRP graph. By the standard mapping,

$$h_i = \frac{w_i}{2} + C, \tag{3}$$

where $w_i$ is the weight function for the $i$-th edge in the graph for a VRP and $C$ is a constant independent of the weight function of the VRP instance $(n, k)$ under consideration. More specifically, $C$ depends on only $n$ and $k$. Thus, the attacker can treat $C$ as a constant offset with the knowledge of $n$ and $k$.

### B. Adding Noise

We introduce noise as imperfect resolution in the rotational angles obtained by the attacker for relevant gates. Taking both noise and variational parameter $\gamma$ into account, for some fixed optimization layer, the rotational angle $\gamma h_i$ associated with $h_i$ can be written as

$$\gamma h_i \pm |\delta h_i| = \gamma \left( \frac{w_i}{2} + C + \frac{\delta h_i}{\gamma} \right). \tag{4}$$

Here, $|\delta h_i|$ is the uncertainty imposed by the noise, upper bounded by the maximum noise magnitude (or maximum imperfection in the resolution). Since the rotational angles fall in the interval $(0, 2\pi]$, the range of maximum noise magnitude we consider is $(0, 2\pi]$.

In our model, we do not assume that the attacker has any information on the variational parameter $\gamma$. In this sense, the variational parameter $\gamma$ acts as an overall normalization factor. Without losing useful information regarding the weight function while cancelling out the constant offset $C$, the attacker can normalize each weight function entry $w_i$ in the following way:

$$\overline{w}_i = \frac{(w_i - w_{\max}) + \frac{2(\delta h_i - \delta h_{\max})}{\gamma}}{(w_{\min} - w_{\max}) + \frac{2(\delta h_{\min} - \delta h_{\max})}{\gamma}}. \tag{5}$$

Here, $w_{\max}$ ($w_{\min}$) is the maximum (minimum) entry in the weight function and $\delta h_{\max}$ ($\delta h_{\min}$) is the corresponding noise. This quantity can be directly obtained both from the weight function as prior knowledge and from empirically obtained rotational angles. As prior knowledge, all noises are set to $0$. Thus, the attacker can compare the set of $\{\overline{w}_i\}$ obtained from the experiments with the precomputed ones to determine the subgraph $G_s$ considered by the victim.

As to the specifics of noise distributions, we consider three distinct types: uniform, bimodal, and Gaussian distributions. For each peak in the Gaussian distributions, we center the peak at $0$ and set the variance such that $> 99.99\%$ of the noise values fall within the maximum noise magnitude. The bimodal distributuions are constructed from the Gaussian distributions, with each peak positioned equidistantly from each other and the noise magnitude boundaries.

### C. General Scheme

A general routine adopted by the attacker can be summarized as follows:

1) For each subgraph $G_s \subseteq G$, precompute the set of normalized weights $\{\overline{w}_i\}_s$.
2) Obtain information on $(n, k)$ and possibly rotational angles from a side-channel attack.
3) Compute a set of $\{\tilde{w}_i\}$ based on the information obtained from the side-channel attack.
4) Compare $\{\tilde{w}_i\}$ with all the precomputed sets of $\{\overline{w}_i\}_s$ and compute the mean squared error (MSE) for each pair.
5) Pick the $G_s$ corresponding to the minimum MSE as the $G_s$ optimized by the victim.

## V. Results and Discussions

In this section, we present our experimental evaluations. Mainly three types of experiments are conducted: matching subgraphs of random sizes under uniform noise, matching subgraphs of fixed sizes under uniform noise, and matching subgraphs of random sizes under different noise types. Note that in all the experiments for matching random subgraphs, we have ignored subgraphs of sizes $\leq 2$, as such subgraphs make the optimization trivial and unnecessary to consider in realistic settings.

In all experiments, we consider both the matching success/error rate and the node recovery proportionality. Here, the matching success/error rate refers to the success/error rate for an attacker to find the complete subgraph that the victim is trying to optimize. However, although an attacker cannot retrieve the complete subgraph sometimes, it is meaningful to consider the portion of the subgraph that the attacker can recover. In this sense, it is useful to consider and evaluate the proportionality of node in a subgraph optimized by the victim recoverable by the attacker.

In Fig. [2, 3, 4], we present the evaluation for the JFK-VRP, a VRP based on the JFK data set described earlier. Due to limited space, we highlight here only results from Fig. [4], where the attacker performs significantly better under Gaussian noise than bimodal and uniform noise. Moreover, the attacker exhibits similar performance under bimodal and uniform noises. To understand this, observe that in the calculation of $\{\overline{w}_i\}_s$, differences between the noises are taken. Since Gaussian noise centers around one peak, the magnitude of this difference is greatly reduced given the small amount of variance under our consideration. We also clarify that except for explicit testing of noise distributions, all the noise distributions adopted in other experiments are of the uniform type.

Below, we list some important observations with concrete statistics based on our experimental results:

- For random subgraphs with size $> 2$, an attacker can stably recover $95\%$ of the nodes and match the entire subgraph correctly with probability $> 0.975$ up to a noise resolution of $\pi/2$.
- For subgraphs of fixed sizes, the larger the subgraph size is, the higher the matching success rate and node recovery proportionality, with both topping at $1.00$ for subgraphs the same size as the mother graph.
- The matching performs better with gaussian noise distributions than bimodal and uniform noise distributions. The advantage grows with noise magnitude, coming to $> 2$ times at large noise.

## VI. Securing VRP

Based on our findings, attackers with access to information about QAOA executing on a quantum computer can recover secrets from the VRP instance. This can compromise secrecy and national security when VRP instances is used in context of routing between army bases or airports. Our work brings particular attention to the need for better understanding, and

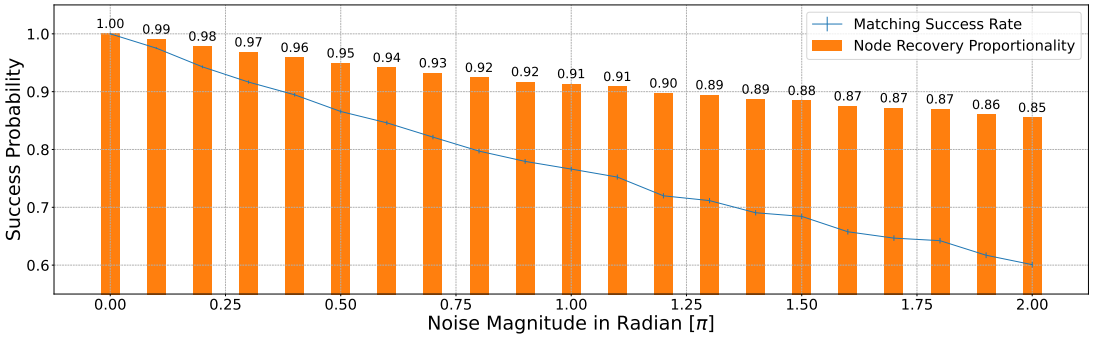


Fig. 2: Experimental evaluations for a strong attacker on matching random subgraphs for JFK-VRP under uniform noise. Both the matching success rate and node recovery proportionality are considered. Maximum noise magnitudes in $(0, 2\pi]$ are evaluated.

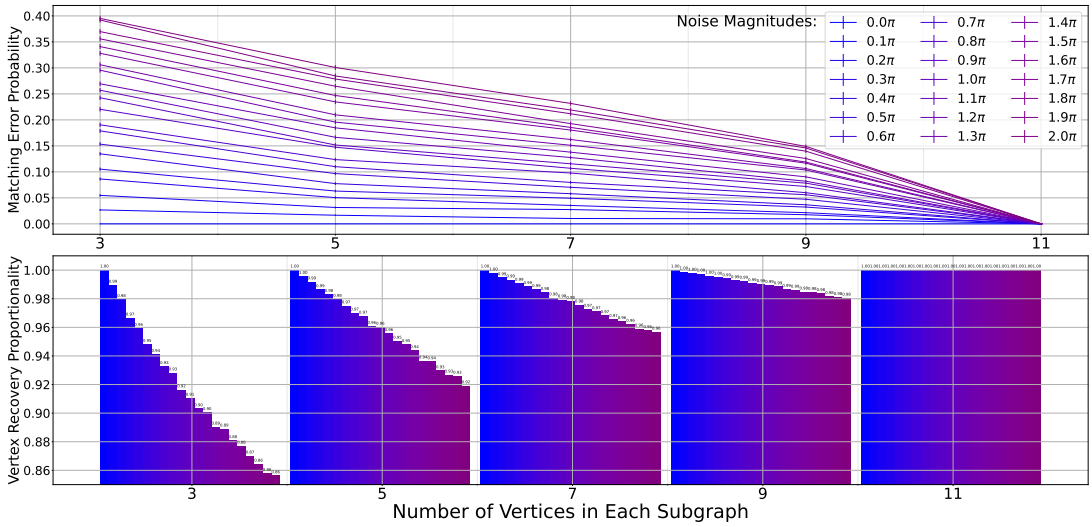


Fig. 3: Experimental evaluations for a strong attacker on matching subgraphs of fixed sizes for JFK-VRP under uniform noise. Both the matching success rate and node recovery proportionality are considered. Maximum noise magnitudes in $(0, 2\pi]$ are evaluated.

prevention, of side channels in quantum computers. As we demonstrate, even imperfect side-channel information corrupted by noise can be leveraged by the attacker. For example, within a noise resolution of $\pi/2$, attackers can stably recover $95\%$ of the nodes and correctly matches the entire subgraph with a probability exceeding $0.85$. As a result, future work needs to explore prevention of side channels, as well as protection of VRP itself.

## VII. Related Work

There is recently, increasingly growing body of research on security of quantum computers. For superconducting quantum computers, recent work [1] shows that the crosstalk errors could be used in fault injection attacks. It also showed how an adversary can launch a denial of service attack on the victim circuit using crosstalk errors, similar to our evaluation. In addition, due to the difference of eigenstates, qubit-sensing employs malicious circuits to sense qubits of victim circuits based on already known statistical information [16]. Among side channel attacks, recent work proposed power side channel attacks that can help recover the control pulses of the quantum computers [22], leading to recovery gates being executed on the quantum computer. Researchers have also proposed different methods to fingerprint quantum computer hardware by characterizing error patterns unique to each device or qubit [11], [14]. In trapped-ion quantum computers, repeated shuttle operations can elevate the ion-chain's energy, which can damage the fidelity of victim circuits [17], [18].

## VIII. Conclusion

This paper focused on an unexplored security domain considering quantum computers: examining the potential compromise of transportation logistics, including civilian airports and military bases, through an analysis of quantum circuit structures. The paper sheds light on how side-channel leaks of information, such as rotational angles, could lead to the recovery of VRP being optimization on a quantum computer. Such breaches carry significant implications for both civilian and national security. The research underscores the urgency in developing robust techniques to safeguard sensitive information, especially in the face of rapid advancements in quantum computing. In particular, it highlights that strong attackers

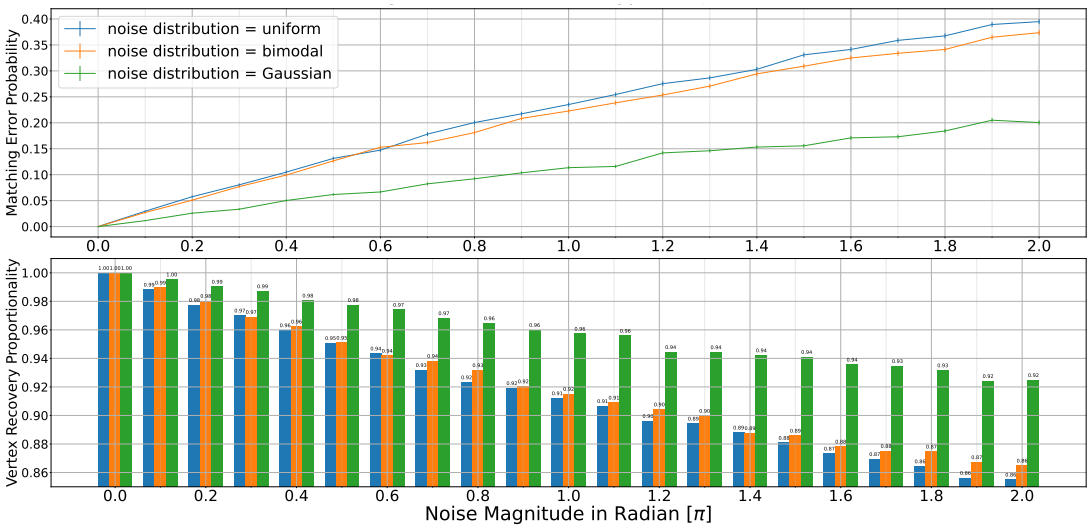


Fig. 4: Experimental evaluations for a strong attacker on matching random subgraphs for JFK-VRP under different noise types: uniform, bimodal and Gaussian. Both the matching success rate and node recovery proportionality are considered. Maximum noise magnitudes in $(0, 2\pi]$ are evaluated.

able to perform side-channel attacks on quantum computing systems pose a nontrivial security threat, emphasizing the need for formulation of effective defense mechanisms to counteract such potential risks.

## REFERENCES


[1] Abdullah Ash-Saki, Mahabubul Alam, and Swaroop Ghosh. Analysis of crosstalk in nisq devices and security implications in multi-programming regime. In *Proceedings of the ACM/IEEE International Symposium on Low Power Electronics and Design*, ISLPED '20, page 25–30, New York, NY, USA, 2020. Association for Computing Machinery.

[2] Utkarsh Azad, Bikash K. Behera, Emad A. Ahmed, Prasanta K. Panigrahi, and Ahmed Farouk. Solving vehicle routing problem using quantum approximate optimization algorithm. *IEEE Transactions on Intelligent Transportation Systems*, 24(7):7564–7573, July 2023.

[3] Sergey Bravyi, David Gosset, and Robert König. Quantum advantage with shallow circuits. *Science*, 362(6412):308–311, October 2018.

[4] Sanjay Deshpande, Chuanqi Xu, Theodoros Trochatos, Hanrui Wang, Ferhat Erata, Song Han, Yongshan Ding, and Jakub Szefer. Design of quantum computer antivirus. In *Proceedings of the International Symposium on Hardware Oriented Security and Trust*, HOST, May 2023.

[5] Nada Elsokkary, Faisal Shah Khan, Davide La Torre, Travis S Humble, and Joel Gottlieb. Financial portfolio management using D-wave quantum optimizer: The case of Abu Dhabi securities exchange, 2017.

[6] Edward Farhi, Jeffrey Goldstone, and Sam Gutmann. A quantum approximate optimization algorithm, 2014.

[7] Sebastian Feld, Christoph Roch, Thomas Gabor, Christian Seidel, Florian Neukart, Isabella Galter, Wolfgang Mauerer, and Claudia Linnhoff-Popien. A hybrid solution method for the capacitated vehicle routing problem using a quantum annealer. *Frontiers in ICT*, 6, June 2019.

[8] FlashGordon. Usa airport dataset. https://www.kaggle.com/datasets/flashgordon/usa-airport-dataset, 2000-2009. Accessed: 2023-11-10.

[9] Harper R. Grimsley, Sophia E. Economou, Edwin Barnes, and Nicholas J. Mayhall. An adaptive variational algorithm for exact molecular simulations on a quantum computer. *Nature Communications*, 10(1), July 2019.

[10] Stuart Hadfield, Zhihui Wang, Bryan O'Gorman, Eleanor Rieffel, Davide Venturelli, and Rupak Biswas. From the quantum approximate optimization algorithm to a quantum alternating operator ansatz. *Algorithms*, 12(2):34, February 2019.

[11] Allen Mi, Shuwen Deng, and Jakub Szefer. Short paper: Device- and locality-specific fingerprinting of shared nisq quantum computers. In *Proceedings of the Workshop on Hardware and Architectural Support for Security and Privacy*, HASP, October 2021.

[12] Allen Mi, Shuwen Deng, and Jakub Szefer. Securing reset operations in nisq quantum computers. In *Proceedings of the Conference on Computer and Communications Security*, CCS, November 2022.

[13] Roman Orus, Samuel Mugel, and Enrique Lizaso. Quantum computing for finance: overview and prospects. *Reviews in Physics*, 4:100028, 2019.

[14] Koustubh Phalak, Abdullah Ash Saki, Mahabubul Alam, Rasit Onur Topaloglu, and Swaroop Ghosh. Quantum puf for security and trust in quantum computing. *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, 11(2):333–342, 2021.

[15] John Preskill. Quantum computing in the nisq era and beyond. *Quantum*, 2:79, August 2018.

[16] Abdullah Ash Saki and Swaroop Ghosh. Qubit sensing: A new attack model for multi-programming quantum computing, 2021.

[17] Abdullah Ash Saki, Rasit Onur Topaloglu, and Swaroop Ghosh. Muzzle the shuttle: Efficient compilation for multi-trap trapped-ion quantum computers, 2021.

[18] Abdullah Ash Saki, Rasit Onur Topaloglu, and Swaroop Ghosh. Shuttle-exploiting attacks and their defenses in trapped-ion quantum computers. *IEEE Access*, 10:2686–2699, 2022.

[19] Maria Schuld, Ilya Sinayskiy, and Francesco Petruccione. An introduction to quantum machine learning. *Contemporary Physics*, 56(2):172–185, 2015.

[20] Ho Lun Tang, V.O. Shkolnikov, George S. Barron, Harper R. Grimsley, Nicholas J. Mayhall, Edwin Barnes, and Sophia E. Economou. Qubit-adapt-vqe: An adaptive algorithm for constructing hardware-efficient ansätze on a quantum processor. *PRX Quantum*, 2(2), April 2021.

[21] Wikipedia contributors. All your base are belong to us — Wikipedia, the free encyclopedia. https://en.wikipedia.org/w/index.php?title=All_your_base_are_belong_to_us&oldid=1189968088, 2023. [Online; accessed 27-December-2023].

[22] Chuanqi Xu, Ferhat Erata, and Jakub Szefer. Exploration of power side-channel vulnerabilities in quantum computer controllers. In *Proceedings of the Conference on Computer and Communications Security*, CCS, November 2023.

[23] Leo Zhou, Sheng-Tao Wang, Soonwon Choi, Hannes Pichler, and Mikhail D. Lukin. Quantum approximate optimization algorithm: Performance, mechanism, and implementation on near-term devices. *Phys. Rev. X*, 10:021067, Jun 2020.

[24] Linghua Zhu, Ho Lun Tang, George S. Barron, F. A. Calderon-Vargas, Nicholas J. Mayhall, Edwin Barnes, and Sophia E. Economou. Adaptive quantum approximate optimization algorithm for solving combinatorial problems on a quantum computer. *Phys. Rev. Res.*, 4:033029, Jul 2022.