SoK: A First Order Survey of Quantum Supply Dynamics and Threat Landscapes

Subrata Das
sjd6366@psu.edu
The Pennsylvania State University
State College, Pennsylvania, USA

Avimita Chatterjee
amc8313@psu.edu
The Pennsylvania State University
State College, Pennsylvania, USA

Swaroop Ghosh
szg212@psu.edu
The Pennsylvania State University
State College, Pennsylvania, USA

ABSTRACT

Quantum computing, with its transformative computational potential, is gaining prominence in the technological landscape. As a new and exotic technology, quantum computers involve innumerable Intellectual Property (IP) in the form of fabrication recipe, control electronics and software techniques, to name a few. Furthermore, complexity of quantum systems necessitates extensive involvement of third party tools, equipment and services which could risk the IPs and the Quality of Service and enable other attack surfaces. This paper is a first attempt to explore the quantum computing ecosystem, from the fabrication of quantum processors to the development of specialized software tools and hardware components, from a security perspective. By investigating the publicly disclosed information from industry front runners like IBM, Google, Honeywell and more, we piece together various components of quantum computing supply chain. We also uncover some potential vulnerabilities and attack models and suggest defenses. We highlight the need to scrutinize the quantum computing supply chain further through the lens of security.

CCS CONCEPTS

• **Security and privacy → Security requirements**; **Hardware attacks and countermeasures**; **Domain-specific security and privacy architectures**.

KEYWORDS

Quantum Computing, Quantum Supply Chain, Intellectual Property, Security Threats, Vulnerabilities

ACM Reference Format:
Subrata Das, Avimita Chatterjee, and Swaroop Ghosh. 2023. SoK: A First Order Survey of Quantum Supply Dynamics and Threat Landscapes. In *Hardware and Architectural Support for Security and Privacy 2023 (HASP '23), October 29, 2023, Toronto, Canada.* ACM, New York, NY, USA, 9 pages. https://doi.org/10.1145/3623652.3623664

1 INTRODUCTION

Quantum computing has the potential to revolutionize fields from cryptography to material science [33, 41]. But beneath the allure lies a complex infrastructure that supports the development, deployment, and operation of quantum computers. This infrastructure, from the fabrication of quantum bits (qubits) and cryogenic control units to the ultra-specific software that governs them, is a vast web of interconnected systems, operations, and technologies [2]. Compared to classical computers, quantum computers are far more complex and require a very close collaboration among material scientists, physicists, engineers from various disciplines and computer scientists, to name a few, to make the system work. These systems are fragile and, as such, require frequent repair, servicing and calibration to maintain their presence in the market. Compared to a classical cloud computing environment where the faulty units can be disabled without a noticeable impact on quality of service (QoS), repair of quantum computers may disrupt the QoS significantly. Therefore, the reliability of the individual components of a quantum computer (besides the quantum processor) is key to maintaining QoS, profit and scientific endeavors. Many companies (who may be leaders in one aspect of quantum computing but not in other areas) are in the race to commercialize their qubit technologies. As such, they are forced to rely on tools and services from third parties not only to reduce the cost but also to bridge the knowledge gap. This situation is very similar to classical integrated circuit (IC) design that relies on third parties for software tools and Intellectual Property (IP) blocks but much exacerbated in the quantum domain.

The supply chain for classical ICs starts with integrating external IP designs with internal designs, validating them and creating the IC layout, often in a GDS-II format [42]. Internal or third party tools are used in the design and validation process. The final layout is sent to a foundry, where a mask is developed, and the ICs are manufactured. The chips are then tested at the manufacturing site and possibly at third-party test facilities. The fault-free chips are packaged, tested and sold. This entire supply chain is spread across multiple countries and hence, can raise security concerns. Therefore, the industry follows a standard procedure for securing the supply chain of classical ICs, which includes measures such as designing with security in mind, collaborating with trusted foundries, rigorous testing, implementing cybersecurity practices, and maintaining transparency.

Although the supply chain of conventional semiconductor technologies has matured over several decades, providing a robust and well-understood foundation, the supply chain for quantum technologies is still in its formative stages. This is primarily due to the fact that classical processors are manufactured in high volume whereas quantum processors are produced at extremely small scale. While specifics might vary between quantum computing architectures (e.g., superconducting qubits [9] versus trapped ions [15]), a general supply chain might look something like Figure 1. Initially,

HASP '23, October 29, 2023, Toronto, Canada

ACM ISBN 979-8-4007-1623-2/23/10…$15.00
https://doi.org/10.1145/3623652.3623664

extensive research is conducted to determine the optimal design and technology. This involves collaboration between scientists and engineers to ensure precision. Companies then choose to either design their own quantum blueprints or acquire pre-existing ones. Specialized materials, of exceptional purity, are procured for the components. Qubits are then fabricated in clean rooms. Following this, quantum processor is integrated with components like control systems and other critical parts to form the quantum computer. These computers require a very low-temperature environment for optimal functionality, necessitating advanced cooling systems. Once assembled, the system undergoes calibration to ensure its components interact correctly. Software is then incorporated, allowing users to interface with and utilize the quantum capabilities. Rigorous testing is carried out to ascertain its readiness. Quantum computers are often accessed remotely via online platforms. Owing to the nascent nature of quantum technology, periodic maintenance and upgrades are essential.

Furthermore, quantum computing systems may include multitude of IPs embedded in various layers of the stack [12, 44]. For example, the real coupling map of the superconducting qubit processor (before disabling the non-functional links), pulsing techniques and frequencies could be an IP. Similarly, the materials used for fabricating the qubits could be an IP. The techniques to suppress crosstalk and noise could also be an IP. At the software level, the techniques to optimize the gate count and circuit depth could represent an IP.

There are known methodologies to protect IPs and establish trust even using untrusted components and parties in classical ICs whereas such methods are not known in the quantum computing domain. The supply chain of quantum computers, software stack, tools and associated services is still evolving. Various companies follow their own supply chain models at their convenience. Companies often employ a mix of in-house facilities for IPs, personalized hardware, or different vendors for components such as dilution refrigerators. Most commonly, companies conduct assembly and testing independently. This lack of standardized clarity within the quantum supply chain exacerbates security risks [12, 48].

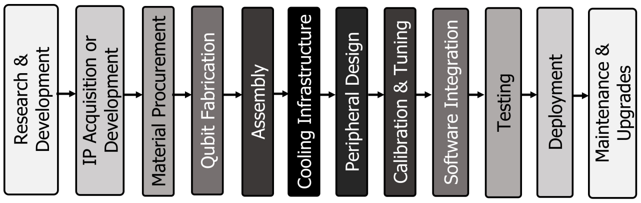

Figure 1: Supply chain of a superconducting quantum computer.

Contributions: We review the design of a representative quantum computing system including hardware, software, firmware, peripherals, and services (Section 2). This is followed by a description of potential IPs embedded in various layers of quantum stack (Section 3). We provide a comprehensive study of the quantum supply chain for prominent companies in the USA synergistic with a recent NSF-OSTP workshop on cybersecurity of quantum computing [36] (Section 4). We also highlight possible vulnerabilities in different layers of the quantum supply chain, attack models and defenses (Section 5). While investigating quantum-specific threats, we underscore that quantum technologies nonetheless inherit many conventional hardware and software vulnerabilities.

2 GENERAL ARCHITECTURE OF A QUANTUM COMPUTER

The architecture of a quantum computer spans from the high-level description of quantum algorithms to the actual physical operation of the qubits. This section will provide an overview of this general architecture (Figure 2) using superconducting quantum computers as an illustrative example.

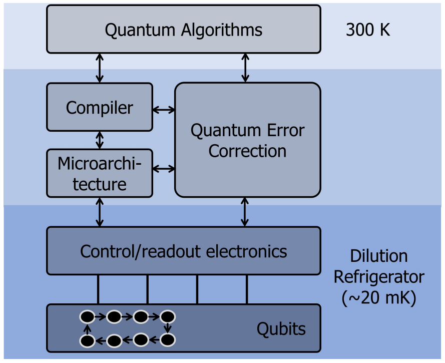

Figure 2: General architecture of a quantum computer. Three blue boxes with color gradients indicate the varying temperature required for different components of the system.

2.1 Quantum Algorithms and Compilers

At the highest level of the quantum computer sits the quantum algorithms, often expressed in a high-level programming language like Q# or Quil. These algorithms operate on idealized logical qubits and gates, without errors [6]. The compiler translates the logical operations into instruction sequences that manipulate the physical qubits to implement the desired algorithms. The compiler schedules and optimizes these circuits while accounting for constraints imposed by qubit connectivity, gate fidelities etc. The pulse sequences and instructions generated by the compiler are then passed to the control electronics, which translate them into analog signals sent to the qubits at precisely timed intervals. Error mitigation and/or correction techniques can be implemented to perform computation in the presence of errors [37].

2.2 Control and Readout Electronics

The operation of quantum computers relies on sophisticated electronics serving two vital roles - control and readout. Control electronics manipulate the quantum processor by sending signals that drive qubit operations. Readout electronics measure the tiny signals produced by the qubits and convert them into usable data. Together, these systems provide the interface between the classical and quantum realms.

For superconducting qubits specifically, control is achieved by applying microwave pulses matched to the frequency of each qubit.

Generating these precise control pulses requires arbitrary waveform generators with sampling rates exceeding 1 GHz to synthesize the pulse envelopes [25]. I/Q (in-phase/quadrature) modulators then provide control over the amplitude, phase, and frequency of a microwave carrier tone. The pulses are combined with the carrier waves through mixers and then up-converted or down-converted to the exact qubit frequencies. Programmable attenuators and amplifiers precisely tune the power levels to ensure accurate qubit manipulation. Switches are used to route pulses to specific qubits as needed. By gating the pulses in time, the switches ensure that operations are only applied to the intended target qubit. Low-frequency control electronics also assist by tuning device parameters and qubit frequencies for optimal performance. Proper coordination of these components enables high fidelity gates operations [26].

Qubit readout starts with faint microwave signals carrying information about the qubit state. Cryogenic amplifiers provide the first stage of amplification, critically boosting signal levels above thermal noise while adding minimal noise themselves [9]. Semiconductor or superconducting parametric amplifiers are often used. Precise timing circuitry triggers the readout process and coordinates the capture of signals. The amplified signal is transmitted outside the cryogenic system for further processing. Additional amplifiers boost the signal, which is then filtered, digitized by high-speed analog-to-digital converters, and processed by digital logic. Field-programmable gate arrays oversee the signal processing, error correction, and integration with control electronics and classical computing resources. Careful calibration ensures high-fidelity qubit readout.

2.3 Qubits

Superconducting quantum computers are composed of superconducting circuits known as qubits, which leverage Josephson junctions (JJ) typically made from thin-film layers of aluminum or niobium. A Josephson junction consists of two superconductors separated by an ultrathin insulating layer. The superconductors contain Cooper pairs, which are bound electrons that enable superconductivity. Cooper pairs can tunnel through the insulating barrier in a Josephson junction, creating a supercurrent flow. This tunneling of Cooper pairs is known as the Josephson effect. The Josephson junction acts as a nonlinear inductive element, where the inductance depends on the supercurrent. When the junctions are cooled below their critical temperature (below 20 mK) they exhibit macroscopic quantum behavior [27]. The quantum state of the junction can be described by a phase variable representing the difference in the quantum mechanical phase between the two superconductors. This phase variable acts as the basis for superconducting qubits. The most common superconducting qubit designs are transmons, flux qubits, and charge qubits. Transmon qubits rely on the nonlinear inductance of Josephson junctions shunted by a large capacitor to make their frequencies insensitive to noise. Flux qubits are composed of a superconducting loop with one or more JJs, where the quantum state depends on the magnetic flux threading the loop. Charge qubits encode information in the charge state of Cooper pairs on a small superconducting island connected to a reservoir via a JJ. These superconducting qubits are fabricated using standard lithographic techniques and deposited in thin film layers on a chip substrate. When cooled to mK temperatures in a dilution refrigerator, they can exist in a quantum superposition and be coherently manipulated by microwave pulses [9].

2.4 Dilution Refrigerator and Associated Controls

To reach the required operating temperatures below 20 mK, the quantum processor is mounted inside a dilution refrigerator. The fridge contains additional wiring, amplifiers, attenuators, filters, and other components to control and interact with the device while minimizing noise [32]. Key components include pulse tube coolers to precool, a mixing chamber where the chip is mounted, and pumps to continuously circulate superfluid helium isotopes (helium-3 and helium-4) to cool the system. Temperature sensors, such as Ruthenium Oxide and Cernox, actively monitor the environment within the fridge, ensuring optimal conditions. Any deviations in temperature are countered by specialized controllers and heaters that adjust based on sensor readings [24]. For experiments demanding specific magnetic field conditions, integrated superconducting magnets, with their own set of control electronics, regulate the strength and direction of the applied field. The system is equipped with mechanisms to counteract the vibrations which can affect the delicate quantum processes. Modern dilution refrigerators also boast software interfaces, facilitating remote monitoring and adjustment, providing researchers with the flexibility to manage operations even from a distance [34].

3 IPS IN THE QUANTUM COMPUTING SYSTEM

IPs in materials and fabrication: Quantum computing is a multifaceted field with many layers, each possessing unique IP aspects. At the heart of quantum computers are the qubits themselves. While companies openly share information about using superconducting circuits or ion traps, the specific materials and composition of these qubits represent closely-guarded trade secrets. For example, IBM publishes research on using transmon qubits made from niobium and aluminum. However, the exact shape, dimensions, treatment, and fabrication of these devices involves proprietary techniques fine-tuned by IBM through years of development [30]. These subtle details can impact qubit performance and reliability, representing the core IP.

IPs in control electronics: Another vital area is qubit control, which relies on precisely tailored microwave pulses applied to each qubit. Companies invest significantly in developing speciality control hardware and custom techniques to manage frequency crowding and prevent crosstalk errors between adjacent qubits. For example, companies may tweak pulse shapes, use optimal control algorithms, or add deliberate frequency offsets to qubits. These are crucial innovations that providers protect through patents and secrecy.

IPs in quantum processor: The qubit connectivity represented by coupling maps is also strategic intellectual property. While providers openly share coupling maps showing how qubits are interconnected, these maps likely differ from the physical hardware itself [36]. Companies may intentionally disconnect or hide certain couplings by disabling them in software. This selective disclosure might be an IP strategy, protecting information that could give insights into a company's unique quantum design [23].

IPs in cooling infrastructure: The operational environment, including the dilution refrigerator, might be customized by each provider to create performance advantages. Companies may modify refrigerators by adding unique wiring, filters, heat shields, and control electronics tailored to their hardware [7]. For instance, they may tweak the mixing chamber shape and materials. The exact configurations, components used, or tweaks made by quantum service providers to these refrigerators can be proprietary, giving them an edge in system stability and performance.

IPs in software and firmware: Quantum compilers often possess proprietary methods for optimizing quantum circuits. Additionally, the strategies used for allocating programs from queues to processors, such as fair share allocation [20], might also contain IPs. However, such specifics can vary depending on the company.

4 QUBIT TECHNOLOGIES & THEIR SUPPLY CHAINS

This section provides a survey of the leading qubit technologies, their implementation, and the key players in the industry. Table 1 compiles essential information on the supply chain infrastructure—including hardware, software, services, peripheral equipment, and firmware—of leading U.S.-based entities operating across diverse qubit platforms. The table further elucidates the specific components employed within these infrastructures and their providers. In instances where specific details regarding a company's supply chain components or providers are not publicly accessible or disclosed, we have denoted these entries within the table using “NA".

4.1 Superconducting Qubits

Superconducting qubits are a leading technology in the field of quantum computing, employed by companies such as IBM, Google, Rigetti Computing, and Bleximo [22].

IBM: IBM's quantum processors, made of superconducting transmon qubits, are housed in Yorktown Heights, New York [17]. Along with their popular quantum software Qiskit, [39], IBM collaborates with other software giants like Zapata Computing, Strangeworks, QxBranch [45]. The dilution fridges are procured from suppliers like Bluefors in Finland and Leiden Cryogenics in the Netherlands [34].

Google: Google's Quantum AI campus is located in California, where they design and develop quantum processors using superconducting qubits [13]. They rely on dilution fridges from Lake Shore Cryotronics situated in Ohio [46].

Rigetti Computing: Rigetti Computing designs and manufactures its quantum processors using superconducting qubits, at their Fab-1 facility in California [40]. The company's recent flagship 84-qubit quantum computer, the Ankaa-1 84-qubit, exemplifies their hardware innovation. These efforts are supported by their own software platform, Forest, including pyQuil, quilc, and QVM [38].

Intel: Intel's exploration into quantum computing encompasses not only superconducting but also spin qubits as a promising alternative [14, 18]. Recently, Intel has made strides with the launch of the “Tunnel Falls" quantum processor [18], housing 12 qubits, a significant step in developing hardware to potentially surpass rivals.

Bleximo: Berkeley-based startup Bleximo specializes in building quantum accelerators and hardware technology for various applications, including cryptography and machine learning [4, 5].

4.2 Trapped Ions

Trapped ions (TI) offer a promising avenue for scalable quantum computing by leveraging the innate properties of ions as qubits. Ions are confined in vacuum chambers using electromagnetic fields, isolating them for manipulation with lasers or microwaves [15]. The key advantage of trapped ions is the Coulombic interaction between them, which refers to the electrostatic force of repulsion between two like electric charges. This Coulombic interaction allows for consistent quantum information transfer and processing between the ions, making multi-qubit operations attainable. The Coulombic force between two trapped ion qubits causes them to "push" apart from each other. However, the electromagnetic trap keeps the ions confined in close proximity. This enables the ions to interact strongly enough that quantum information can be exchanged between them through their motion, while still being isolated from external noise sources.

Honeywell: Honeywell Quantum Solutions, based in Colorado, specializes in TI quantum computing, using ytterbium ions as qubits [16]. They have created a 10-qubit quantum computer with plans to reach 100 qubits by 2024. Honeywell has also devised quantum software tools, including a compiler and error correction software.

IonQ: IonQ, headquartered in Maryland, is at the forefront of TI technology in quantum computing [19]. IonQ Forte, the world's first software-configurable quantum computer, utilizes ytterbium ions and advanced acousto-optic deflectors (AODs) for precision and adaptability.

Alpine Quantum Technology: Alpine Quantum technology captures single-charged atoms within vacuum chambers using electric fields, turning each atom into a qubit, which is then precisely manipulated with laser pulses [3].

4.3 Topological Qubits

Topological qubits present an intriguing pathway in quantum computing, utilizing topological states of matter to encode and protect quantum information. Unlike traditional qubits, topological qubits leverage the braiding of exotic particles like anyons and Majorana fermions, rendering them naturally resilient to local noise and disturbances [31].

Microsoft: Microsoft's foray into topological quantum computing focuses on Majorana fermions, particles not yet definitively observed but promising for error resilience [29]. Their Quantum Lab at the University of California, Santa Barbara, has developed specialized cryogenic systems and fabrication processes.

4.4 Photonics-Based Quantum Computing

Photonics-based quantum computing centers on modulating individual photon states to execute quantum functionalities, encompassing phenomena like superposition and entanglement [43]. Generated primarily by lasers, these photons traverse through an assembly of optical components like beamsplitters, phase shifters and

Table 1: The Quantum Industry Map

Qubit Technology	Company	Infrastructure	Components	Provider
Superconducting Qubits	**IBM**	Hardware	Qubits/Quantum processors	IBM Research Center
		Software	Compiler/Qiskit	IBM; other partners.
		Services	Calibration	IBM Quantum Support
		Peripheral	Dilution fridge	Bluefors and Leiden Cryogenics
		Firmware	Control electronics	IBM
	Google	Hardware	Qubits/Quantum processors	Google Research
		Software	QC Software Framework/Cirq	Google
		Services	Quantum Cloud Services	Google Cloud Platform
		Peripheral	Dilution fridge	Lake Shore Cryotronics
		Firmware	NA	NA
	Rigetti Computing	Hardware	Qubits/Quantum processors	Rigetti Computing
		Software	Quantum Computing Software	Rigetti Computing
		Services	Quantum Cloud Services	Rigetti Quantum Cloud Services
		Peripheral	Dilution fridge	Bluefors
		Firmware	NA	NA
	Intel	Hardware	Superconducting & Spin qubits	Intel
		Software	Intel Quantum Simulator	
		Services	NA	NA
		Peripheral	Dilution fridge, Cryogenic Control Systems (Horse Ridge)	Bluefors, Intel, QuTech
		Firmware	NA	NA
	Bleximo	Hardware	Quantum accelerators	Bleximo
		Software	Quantum Computing Software	
		Services	Calibration/Training/Support	
		Peripheral	Dilution fridge	Bluefors, Oxford Instruments
		Firmware	Control stack	Bleximo
Trapped Ions	**Honeywell**	Hardware	Qubits/Quantum processors	Honeywell Quantum Solutions
		Software	Quantum software tools	
		Services	Access, consulting & collaboration	
		Peripheral	Cryogenic equipment	
		Firmware	NA	NA
	IonQ	Hardware	Qubits/Quantum processors	IonQ
		Software	Compiler/IonQ Cloud	IonQ; other partners
		Services	Calibration/Support	IonQ Quantum Support
		Peripheral	Cryogenic control electronics and vacuum hardware	IonQ
		Firmware	NA	NA
Topological Qubits	**Microsoft**	Hardware	Topological qubits	Microsoft's QC Lab
		Software	Q# language, QDK	Quantum Architectures and Computation Group
		Services	Optimization, enterprise-grade security, hybrid cloud	Microsoft Azure Quantum
		Peripheral	Dilution refrigerators	Microsoft's QC Lab
		Firmware	NA	NA
Photonics Based Quantum Computing	**XANADU AI**	Hardware	Borealis, X-Series	Xanadu
		Software	PennyLane, Strawberry Fields	
		Services	Lightning, Jet simulators, Cloud	
		Peripheral	NA	NA
		Firmware		
Quantum Annealing Based Quantum Computing	**D-Wave**	Hardware	Qubits/Quantum processors	D-Wave Systems
		Software	Ocean software development kit	
		Services	Leap quantum cloud service	
		Peripheral	Cryogenic equipments	Various suppliers
		Firmware	NA	NA

detectors. Key players like Xanadu, ORCA Computing, PsiQuantum, TundraSystems Global, Quandela, and QuiX Quantum are actively driving research and development in this field [8].

XANADU AI: Xanadu AI, headquartered in Canada, has developed hardware, particularly the Borealis and X-Series, which utilize photon-based squeezed state qubits [47]. Xanadu also offers the PennyLane software development kit coupled with Strawberry Fields—a groundbreaking open-source library curated for quantum machine learning [35].

4.5 Quantum Annealing

Quantum annealing is a sophisticated computational approach to address optimization challenges [21]. Unlike classical methods that examine one solution at a time, quantum annealing, with the help of superposition, explores a multitude of potential solutions simultaneously, leading to swifter convergence to the most optimal one.

D Wave & Fujitsu: D-Wave Systems, based in British Columbia, has innovated multiple quantum annealing systems, with the D-Wave Advantage2 being their most advanced release. These systems, known as D-Wave Quantum Processing Units (QPUs), utilize superconducting circuits to execute quantum annealing operations. D-Wave also offers the Ocean software development kit. Leap™ quantum cloud service provides enhanced accessibility to their quantum computing resources.[10]

Fujitsu has developed Digital Annealer [11] which is a classical system equipped with a unique processor designed to emulate quantum annealing behaviors.

5 QUANTUM SUPPLY CHAIN SECURITY

5.1 Leakage of IP

From Table 1, it is evident that quantum computing systems may involve many third parties. This could present a risk to the IPs embedded in various layers of the stack. For example, calibration service providers may have access to the control electronics and pulsing and error mitigation strategies. Such information could be valuable to competitors and may be subject to leakage. Similarly, dilution fridge provider may have access to the quantum processor and the physical coupling map. Users have access to the compiler and the backends via APIs (Application Programming Interface). Although not shown, one can reverse engineer various compilation policies from access to the compiler.

There are several ways IP could potentially be leaked across the quantum technology stack through third party partners. At the materials and fabrication level, insider theft or cyber intrusions could compromise proprietary techniques for producing high-quality qubits, giving competitors valuable insights into optimizing qubit coherence times. Partners involved in calibration and servicing of control electronics may gain access to sensitive pulse parameters, firmware details, and error mitigation strategies that could improve competitor fidelities if leaked. Dilution refrigerator partners may learn layout and wiring tricks that help reduce noise and optimize qubit performance. Access to compilers provides opportunities for software IP leakage around circuit optimization and mapping techniques. Additionally, partners seeing the firmware and peripherals used in control and readout electronics could copy techniques for pulse generation, timing calibration etc. if not properly secured. Algorithm partners may also deduce scheduling policies for queuing and resource allocation that provide competitive advantages. Potential vectors through which proprietary IP could be leaked include insider theft at partner facilities, data exfiltration through cyber intrusions of collaborator systems, reverse engineering of legitimately obtained systems or products, social engineering to extract information from authorized users, and improper handling of IP without proper access controls.

5.2 QoS degradation

Quantum computers rely on sophisticated peripherals like control/readout electronics, and cryogenic systems. Faults in these components can disrupt operations and reduce uptime. For example, a faulty microwave pulse generator that controls qubit gates would halt operations until fixed, severely impacting the QoS. Unlike classical cloud infrastructure, where redundancies provide resilience, most quantum providers operate singular, specialized systems with limited backup. These are highly specialized and customized systems involving unique qubit chips, control electronics, and peripheral equipment tailored for that particular device. Unlike classical cloud infrastructure, quantum systems do not have redundant backup systems readily available. This lack of swappable redundant quantum computers makes quantum systems far more vulnerable to supply chain disruptions than classical computing. Furthermore, hardware supply chain issues such as recycled and tampered parts can cause deliberate faults and leak information.

5.3 Other Possible Attack Scenarios

Hardware Weaknesses and Sensitivities: The intricate quantum supply chain provides multiple avenues for potential manipulation of hardware properties by adversaries like malicious service providers with internal access. Firstly, qubits' fidelity and coherence time depends heavily on precise ambient conditions like temperature, noise, and magnetic shielding, which could be maliciously perturbed. Introducing even small controlled disturbances to these parameters, by compromising any part of the supply chain (e.g., untrusted parts within dilution refrigerator) responsible for maintaining these conditions, could deteriorate qubit performance. This can also create detectable changes in timing or power side-channels that attackers could exploit to extract information such as user circuits or even reconstruct the full algorithm [48]. Furthermore, properties like qubit connectivity, gate errors, and crosstalk are characterized during hardware calibration and testing before deployment. This data on error rates and qubit behavior is used when compiling and mapping quantum circuits onto the physical qubits. Maliciously altering such data can cause the compiler to make suboptimal or incorrect mapping decisions, assigning logical qubits to physical qubits differently [1].

Peripheral Infiltration: The peripherals like dilution refrigerators and control/readout electronics in the quantum stack also present potential attack surfaces. For instance, the extreme cooling and isolation provided by fridges are critical for superconducting qubits [24]. Manipulation of fridge wiring or components by a compromised/malicious supplier could degrade qubit performance. Even minor changes to thermal regulation or noise filtering could kick qubits out of their fragile operating zones and open side-channels. Additionally, control electronics that generate microwave pulses rely on precise timing and synchronization. Small deviations by exploiting peripherals like arbitrary waveform generators, switches, or attenuators could corrupt pulse shapes. This can fail operations and create detectable anomalies for attackers to exploit. Further, any backdoors or kill switches introduced at the peripheral level could disable systems or wreck havoc at critical moments. The readout electronics are also susceptible. They amplify and process qubit measurements, which could be altered by compromising cryogenic amplifiers or ADC converters. Readout manipulation would corrupt program outputs. Sabotaged interconnects between peripherals could also disconnect vital components like amplifiers or magnets needed for qubit control.

Firmware Threats: The myriad firmware across the quantum stack also poses risks if compromised. For instance, control electronics use FPGAs running low-level firmware to coordinate qubit manipulations. Inserting backdoors could allow attackers to corrupt/manipulate pulse generation. Subtle perturbations to pulse parameters through firmware bugs can degrade fidelity enough to create side-channels. Refrigerator firmware that regulates qubit environment could similarly be targeted. Bugs inducing even small temperature or vibration changes may push qubits out of their operating sweet spot. Qubit calibration firmware also holds value and could be a target. Altering calibration could cripple performance or aid side-channels.

Software Vulnerabilities: The intricate software stack supporting quantum computers presents multiple potential attack surfaces if compromised. Quantum algorithms initially expressed in high-level languages are compiled down to low-level pulse sequences executed on hardware. Inserting vulnerabilities during compilation could corrupt pulse parameters or scheduling in hard-to-detect ways. For example, a compromised compiler could manipulate gate decomposition or qubit mapping to degraded fidelity while maintaining functional correctness [12]. In addition to the compiler, software is responsible for orchestrating execution of user programs on quantum systems. This includes queuing submitted programs and allocating available quantum resources between users. The algorithms governing this scheduling and allocation could be manipulated to give certain users preferential treatment. For example, a backdoor in the scheduling software could allow specific users to jump ahead/behind in the queue or receive more/less processing time on quantum hardware. Therefore, some users could monopolize the system while denying services to others. Since quantum computer time is extremely limited, even small advantages in scheduling can be impactful. Furthermore, flaws in the design of APIs used to interface with quantum cloud platforms may exist. Attackers who discover these flaws could exploit the APIs to extract sensitive data about internal architectures or gain elevated privileges. Common API vulnerabilities like buffer overflows, command injections, or lack of input validation could allow adversaries to crash systems, manipulate outputs, or exfiltrate information. Additionally, quantum access is often provided via cloud-based services. Insufficient encryption and access controls on these cloud platforms further increase the attack risk. Attackers may intercept data, steal credentials, or gain persistence in cloud systems housing quantum software infrastructure [44].

A recent work has demonstrated how measurement errors in multi-tenant quantum computers can enable information leakage between users [28]. For example, an adversary could run ancilla qubits in parallel with a victim's computation. By measuring the ancilla qubits, the adversary can estimate the state of the victim's qubits which may contain sensitive results. This exploits the correlation between measurement errors on neighboring qubits. By repeating this attack, the adversary can recover partial to full information about the victim's outputs. Such measurement-based interference poses a threat in multi-user settings if qubits are not securely reset between users.

5.4 Defense Strategies

Safeguarding the quantum supply chain requires multilayered defenses and controls spanning people, processes, components and technology. For personnel (including external third party service providers), the usual screening, background checks and contractual terms can prohibit leakage of proprietary information. Multi-party computation protocols may allow collaborative development without full IP disclosure. Process-wise, supplying vendors with only the minimal necessary data can reduce exposure. Regular audits can validate that proper controls and procedures are in place. Technology protections include obfuscation, access restrictions, data encryption, and watermarking IP to track dissemination. Formal verification of compiled code or firmware and enforcement of best code writing practices can protect from vulnerabilities that can enable code injection.

To mitigate hardware weaknesses, providers can perform continuous runtime monitoring and anomaly detection on critical parameters like temperature, noise, vibrations to catch any deviations from expected ranges. Redundant sensors can validate readings. Tamper-resistant packaging and authenticated firmware updates can prevent malicious modifications to peripherals. Authentication mechanisms can ensure only trusted certified hardware is integrated into systems. Defenses for peripherals involve following secure hardware design practices like isolating components, encrypted programming interfaces, and internal monitoring for abnormal behavior. Providers can collaborate with reputable, audited vendors to reduce supply chain risks. Cryptographically signing firmware and continuously validating peripherals firmware through secure boot mechanisms can prevent backdoors. Monitoring power profiles can catch anomalies in pulse generation or timing that could signal an attack.

To secure firmware across the stack, code should be formally verified before deployment and written following best practices to avoid vulnerabilities. Runtime attestation can continually validate firmware integrity and catch unauthorized modifications. Segmenting and sandboxing firmware components can limit the impact of any single compromise. Secure encrypted update mechanisms ensure only legitimate authorized firmware approved by the provider can be flashed onto devices. Software protections include developer training, following secure coding standards, and extensive testing/auditing before release. Compartmentalizing software modules and strictly limiting inter-module communication via authentication and encryption can contain breaches. Continuously monitoring for abnormal behavior during runtime can catch attacks. Providers can encrypt code binaries and use code obfuscation to prevent reverse engineering. Securing cloud APIs requires rigorous penetration testing, input sanitization, and restricting API functionality to least privilege.

There is also a need for defenses like the secure reset operation to prevent retaining qubit state that could propagate errors enabling measurement-based interference attacks between users in multi-tenant settings [28]. By randomly inserting reset operations and ensuring their uniform timing, a secure reset scheme can limit the amount of usable information that could leak between qubits across user boundaries.

To minimize disruptions from faulty components and improve QoS, rigorous screening of parts and stress testing can be done. Redundant spares will allow rapid swap-in to restore services. Fail-safe designs may prevent single points of failure, and live redundancy techniques can provide constant backup systems. For quick recovery, effective repair management and supply processes are needed to enable prompt part replacement. Obfuscation to mask power or timing can address potential side channel leakages. To ensure reliable quantum computing with an unreliable or untrusted supply chain, one can continuously monitor and verify the integrity of critical components during operation. Additionally, using checksums, challenge-response protocols, and anomaly detection can help identify compromised components in real-time.

6 CONCLUSIONS

We presented a first order analysis of quantum computing supply chain covering a wide range of qubit technologies. After reviewing the architecture of a representative quantum computing system, we presented various potential IPs embedded in various layers of the quantum stack. We also uncovered several potential security issues that have striking similarities with classical computing such as leakage of IP, QoS degradation and peripheral/software/firmware level attacks and a direction for defenses. Our study highlights the need to scrutinize the supply chain of quantum computers further to uncover potential vulnerabilities and threats and to build defenses proactively.

ACKNOWLEDGMENTS

The work is supported in parts by the National Science Foundation (NSF) (CNS-1722557, CCF-1718474, OIA-2040667, DGE-1723687 and DGE-1821766).

REFERENCES

[1] Nikita Acharya and Samah Mohamed Saeed. 2020. A lightweight approach to detect malicious/unexpected changes in the error rates of NISQ computers. In *Proceedings of the 39th International Conference on Computer-Aided Design*. 1–9.

[2] Garrelt JN Alberts, M Adriaan Rol, Thorsten Last, Benno W Broer, Cornelis C Bultink, Matthijs SC Rijlaarsdam, and Amber E Van Hauwermeiren. 2021. Accelerating quantum computer developments. *EPJ Quantum Technology* 8, 1 (2021), 18.

[3] AQT 2023. *AQT Technology*. Retrieved August 13, 2023 from https://www.aqt.eu/technology/

[4] Bleximo. 2022. *Cryogenic Hardware at Bleximo: Superconducting Quantum Processor Packaging and Shielding*. Retrieved August 13, 2023 from https://medium.com/bleximo/cryogenic-hardware-at-bleximo-superconducting-quantum-processor-packaging-and-shielding-d0d2b84b47d3

[5] Bleximo 2023. *Powering Innovation Through Quantum Computing*. Retrieved August 13, 2023 from https://bleximo.com/

[6] Andrew W Cross, Lev S Bishop, John A Smolin, and Jay M Gambetta. 2017. Open quantum assembly language. *arXiv preprint arXiv:1707.03429* (2017).

[7] James A Crunkleton. 1992. *Cryogenic refrigeration apparatus*. Technical Report. Boreas Inc.

[8] James Dargan. 2022. *81 Quantum Computing Companies: An Ultimate 2023 List*. Retrieved August 13, 2023 from https://thequantuminsider.com/2022/09/05/quantum-computing-companies-ultimate-list-for-2022/

[9] Michel H Devoret and Robert J Schoelkopf. 2013. Superconducting circuits for quantum information: an outlook. *Science* 339, 6124 (2013), 1169–1174.

[10] DWave 2023. *How D-Wave Systems Work* . Retrieved August 13, 2023 from https://www.dwavesys.com/learn/quantum-computing/

[11] Fujitsu 2023. *Fujitsu Digital Annealer*. Retrieved August 13, 2023 from https://www.fujitsu.com/global/services/business-services/digital-annealer/

[12] Swaroop Ghosh, Suryansh Upadhyay, and Abdullah Ash Saki. 2023. A Primer on Security of Quantum Computing. *arXiv preprint arXiv:2305.02505* (2023).

[13] GoogleQuantumLab 2023. *Google Quantum AI: Our Lab*. Retrieved August 13, 2023 from https://quantumai.google/hardware/our-lab

[14] Gian Giacomo Guerreschi, Justin Hogaboam, Fabio Baruffa, and Nicolas P D Sawaya. 2020. Intel Quantum Simulator: a cloud-ready high-performance simulator of quantum circuits. *Quantum Science and Technology* 5, 3 (may 2020), 034007. https://doi.org/10.1088/2058-9565/ab8505

[15] Hartmut Häffner, Christian F Roos, and Rainer Blatt. 2008. Quantum computing with trapped ions. *Physics reports* 469, 4 (2008), 155–203.

[16] Honeywell 2023. *Honeywell Quantum*. Retrieved August 13, 2023 from https://www.honeywell.com/us/en/company/quantum

[17] IBM Quantum 2023. *IBM Quantum Computing Research*. Retrieved August 13, 2023 from https://research.ibm.com/quantum-computing

[18] Intel 2023. *Intel Quantum Computing*. Retrieved August 13, 2023 from https://www.intel.com/content/www/us/en/research/quantum-computing.html

[19] IonQ 2023. *IonQ Technology*. Retrieved August 13, 2023 from https://ionq.com/technology

[20] Toshinari Itoko and Takashi Imamichi. 2020. Scheduling of operations in quantum compiler. In *2020 IEEE International Conference on Quantum Computing and Engineering (QCE)*. IEEE, 337–344.

[21] Tadashi Kadowaki and Hidetoshi Nishimori. 1998. Quantum annealing in the transverse Ising model. *Physical Review E* 58, 5 (1998), 5355.

[22] Morten Kjaergaard, Mollie E Schwartz, Jochen Braumüller, Philip Krantz, Joel I-J Wang, Simon Gustavsson, and William D Oliver. 2020. Superconducting qubits: Current state of play. *Annual Review of Condensed Matter Physics* 11 (2020), 369–395.

[23] Mauritz Kop, Mateo Aboy, and Timo Minssen. 2022. Intellectual property in quantum computing and market power: a theoretical discussion and empirical analysis. *Journal of Intellectual Property Law and Practice* 17, 8 (2022), 613–628.

[24] Sebastian Krinner, Simon Storz, Philipp Kurpiers, Paul Magnard, Johannes Heinsoo, Raphael Keller, Janis Luetolf, Christopher Eichler, and Andreas Wallraff. 2019. Engineering cryogenic setups for 100-qubit scale superconducting circuit systems. *EPJ Quantum Technology* 6, 1 (2019), 2.

[25] Yao Lu, Srivatsan Chakram, Ngainam Leung, Nathan Earnest, Ravi K Naik, Ziwen Huang, Peter Groszkowski, Eliot Kapit, Jens Koch, and David I Schuster. 2017. Universal stabilization of a parametrically coupled qubit. *Physical review letters* 119, 15 (2017), 150502.

[26] Erik Lucero, Max Hofheinz, Markus Ansmann, Radoslaw C Bialczak, N Katz, Matthew Neeley, AD O'Connell, H Wang, AN Cleland, and John M Martinis. 2008. High-fidelity gates in a single Josephson qubit. *Physical review letters* 100, 24 (2008), 247001.

[27] John M Martinis, Ken B Cooper, Robert McDermott, Matthias Steffen, Markus Ansmann, KD Osborn, Katarina Cicak, Seongshik Oh, David P Pappas, Raymond W Simmonds, et al. 2005. Decoherence in Josephson qubits from dielectric loss. *Physical review letters* 95, 21 (2005), 210503.

[28] Allen Mi, Shuwen Deng, and Jakub Szefer. 2022. Securing Reset Operations in NISQ Quantum Computers. In *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security*. 2279–2293.

[29] Microsoft 2015. *The Quantum Quest at Microsoft*. Retrieved August 13, 2023 from https://www.microsoft.com/en-us/research/blog/the-quantum-quest-at-microsoft/

[30] Masoud Mohseni, Peter Read, Hartmut Neven, Sergio Boixo, Vasil Denchev, Ryan Babbush, Austin Fowler, Vadim Smelyanskiy, and John Martinis. 2017. Commercialize quantum technologies in five years. *Nature* 543, 7644 (2017), 171–174.

[31] Chetan Nayak, Steven H Simon, Ady Stern, Michael Freedman, and Sankar Das Sarma. 2008. Non-Abelian anyons and topological quantum computation. *Reviews of Modern Physics* 80, 3 (2008), 1083.

[32] C Neill, A Megrant, R Barends, Yu Chen, B Chiaro, J Kelly, JY Mutus, PJJ O'Malley, D Sank, J Wenner, et al. 2013. Fluctuations from edge defects in superconducting resonators. *Applied Physics Letters* 103, 7 (2013).

[33] Michael A Nielsen and Isaac L Chuang. 2001. Quantum computation and quantum information. *Phys. Today* 54, 2 (2001), 60.

[34] Dan O'Shea. 2021. *IBM-Bluefors partnership promises really cool quantum future*. Retrieved August 13, 2023 from https://www.insidequantumtechnology.com/news-archive/ibm-bluefors-partnership-promises-really-cool-quantum-

future/

[35] PennyLane Website 2023. *PennyLane*. Retrieved August 13, 2023 from https://pennylane.ai/

[36] Pittsburg Quantum Institute 2023. *Workshop on Cybersecurity of Quantum Computing*. Retrieved August 13, 2023 from https://www.pqi.org/news/workshop-cybersecurity-quantum-computing

[37] John Preskill. 2018. Quantum computing in the NISQ era and beyond. *Quantum* 2 (2018), 79.

[38] PyQuil 2023. *PyQuil Documentation*. Retrieved August 13, 2023 from https://pyquil-docs.rigetti.com/en/v2.7.2/

[39] Qiskit 2023. *Qiskit*. Retrieved August 13, 2023 from https://qiskit.org/

[40] Rigetti 2023. *Rigetti: What We Build*. Retrieved August 13, 2023 from https://www.rigetti.com/what-we-build

[41] Michiel Adriaan Rol. 2020. Control for programmable superconducting quantum systems. (2020).

[42] Masoud Rostami, Farinaz Koushanfar, and Ramesh Karri. 2014. A primer on hardware security: Models, methods, and metrics. *Proc. IEEE* 102, 8 (2014), 1283–1295.

[43] Shuntaro Takeda and Akira Furusawa. 2019. Toward large-scale fault-tolerant universal photonic quantum computing. *APL Photonics* 4, 6 (2019).

[44] Theodoros Trochatos, Chuanqi Xu, Sanjay Deshpande, Yao Lu, Yongshan Ding, and Jakub Szefer. 2023. Hardware Architecture for a Quantum Computer Trusted Execution Environment. *arXiv preprint arXiv:2308.03897* (2023).

[45] Jeff Wesler. 2018. *IBM Collaborating With Top Startups to Accelerate Quantum Computing*. Retrieved August 13, 2023 from https://newsroom.ibm.com/IBM-research?item=30420

[46] Kyle Wiggers. 2019. *Google's new cryogenic quantum controller uses less than 2 milliwatts*. Retrieved August 13, 2023 from https://venturebeat.com/mobile/googles-new-cryogenic-quantum-controller-uses-less-than-2-milliwatts/

[47] Xanadu Website 2023. *Xanadu*. Retrieved August 13, 2023 from https://www.xanadu.ai/

[48] Chuanqi Xu, Ferhat Erata, and Jakub Szefer. 2023. Exploration of Quantum Computer Power Side-Channels. *arXiv preprint arXiv:2304.03315* (2023).