Trapped Ion Quantum Computing: A Framework for Addressing Security Vulnerabilities

Karli E. Wallace, Leleia A. Hsia and Mark G. Reith
Air Force Institute of Technology, Dayton, OH, USA

Karli.Wallace.1@au.af.edu
Leleia.Hsia.2@au.af.edu
Mark.Reith.3@au.af.edu

Abstract: Trapped ion quantum computing has the potential to revolutionize computational paradigms. As the adoption of this technology grows, so does the need for stringent scrutiny of its involvement in cybersecurity, especially when it has implications in national defense or critical infrastructure. While trapped ion quantum computing offers transformative capabilities, it is vital to carefully examine the potential vulnerabilities associated with its use and patch them before implementing this powerful technology. In this paper, we examine the potential vulnerabilities in trapped ion quantum computing systems and propose a framework for addressing them. This framework includes risk assessment for evaluating vulnerabilities, threat modeling for identifying exploits, and prevention and mitigation for reducing their impact.

Keywords: Quantum Computing, Trapped Ion, Cybersecurity, Threat Modeling, Risk Assessment Framework

1. Introduction

Over the past few years, quantum computing has gained much-deserved attention for its potential to revolutionize computational paradigms. At the forefront of this technology, trapped ion quantum computing has the power to harness the principles of quantum mechanics to process information in ways unattainable by traditional computers. Trapped ion computers manipulate confined ions through electromagnetic fields. This approach offers distinct advantages, including high-fidelity quantum bit operations and long coherence times, both of which are necessary for maintaining the quantum states needed for computations. However, as the development of trapped ion technology gains momentum, it is imperative to incorporate robust cybersecurity into its architecture, especially when it is integrated into national defense and critical infrastructure. This paper proposes a framework to address the vulnerabilities in this technology to maintain the strategic advantages in a quantum-enabled world.

2. Background

2.1 Concepts of Quantum Computing

Quantum computing represents a significant leap in the field of computation. It utilizes the principles of quantum theory, which governs the behavior of energy and material on the atomic and subatomic levels. Unlike classical computing, which relies on bits that exist as either 0 or 1, quantum computing (QC) uses quantum bits, also called qubits. These qubits can exist in multiple states simultaneously thanks to the principle of superposition (Herman and Friedson, 2018). Superposition allows a qubit to be in a combination of both 0 and 1 states at the same time, drastically increasing the computational power of quantum computers over classical computers. Furthermore, QC takes advantage of the principle of entanglement, which enables multiple qubits to be in a correlated state, where the state of one (whether in superposition or not) can depend on the state of another, no matter how far apart they are.

These fundamental differences grant quantum computers the potential to process complex problems considered intractable for classical computers. For tasks like cryptography, material science simulations, and complex algorithm solving (Murali et al., 2020), QC offers a promising future. However, the technology is still in its nascent stages, and practical, large-scale quantum computers are yet to be fully realized. Some of the obstacles still being addressed are the sensitivity of qubits and the challenge of maintaining their state without decohering due to disturbance from their environment (Herman and Friedson, 2018). Despite these challenges, the progress in QC hints at a revolutionary change in how we approach complex computational problems.

2.2 Trapped Ion Quantum Computing Technology

Trapped ion quantum computing technology is one of the leading approaches in the development of quantum computers. This method involves trapping charged ions in a controlled environment with electromagnetic fields (Bruzewicz et al., 2019). In trapped ion (TI) QC, qubits are represented by the quantum states of these ions, which are manipulated using lasers. The precision of laser control allows for the execution of quantum gates and operations necessary for QC. One of the key advantages of TI technology is its high fidelity in qubit manipulation and relatively long coherence times (Bruzewicz et al., 2019), which are crucial for maintaining the quantum state of the system.

The current state of TIQC in the market is still in an early phase consisting of ongoing research and development. Currently, companies like IonQ and Honeywell are at the forefront of commercializing TIQC technology (Herman and Friedson, 2018). In particular, IonQ has made significant strides in developing quantum computers that are accessible through cloud platforms and partnering with major tech companies to integrate QC into various industries (IonQ | Trapped Ion Quantum Computing, no date)(Hassija et al., 2020). Honeywell has also been actively investing in and developing its own TIQC solutions (Hassija et al., 2020) (Get to Know Honeywell's Latest Quantum Computer System Model H1, no date).

These developments indicate a growing interest and investment in TI technology in the QC market. While the realization of large-scale commercial applications may still be years away, the continuous advancements in TI are paving the way for more robust and scalable QC solutions in the future.

2.3 Cybersecurity and National Defense

The emergence of QC brings a paradigm shift in cybersecurity, especially within the realm of national defense. The potential for QC to break current encryption standards poses a significant challenge to the security of sensitive data and critical infrastructure (Phalak et al., 2021). Countries and defense agencies worldwide are increasingly focusing on quantum-resistant algorithms and encryption methods to safeguard against the threat posed by QC capabilities (Herman and Friedson, 2018). This includes developing new cryptographic standards that can withstand quantum attacks, a field known as post-quantum cryptography (Murali et al., 2020). The race to achieve quantum supremacy is not just about increasing computational power but also about improving security and maintaining strategic advantages in national defense. This makes the race to quantum supremacy a top priority for governments and defense agencies worldwide.

In the context of national defense, the importance of computational technology cannot be overstated. Critical infrastructure, including communications networks, power grids, and defense systems, rely heavily on secure data transmission and storage (Phalak et al., 2021). The emergence of QC requires the reevaluation of current cybersecurity protocols in these areas to prevent potential breaches that could compromise national security. Defense departments are investing in QC partly to develop new post-quantum security measures, and partly to anticipate the potential offensive capabilities of adversaries who might use QC to break encryptions (Phalak et al., 2021). Additionally, QC offers unique advantages in secure communications, notably through quantum key distribution (QKD), which provides a theoretically unbreakable encryption method (Phalak et al., 2021). QKD ensures that any eavesdropping attempt can be detected since observing the quantum state of a particle invariably alters the state.

3. Identify Vulnerabilities in Trapped Ion Quantum Computing

While identifying vulnerabilities in trapped ion quantum computing systems, it is important to examine both hardware- and software-level components. An overview of this examination can be seen in Table 1 (Herman and Friedson, 2018).

3.1 Hardware

On the hardware front, TI quantum computers rely on intricately designed and highly sensitive components to trap and manipulate ions (Saki et al., 2021). These components include ion traps, lasers, and detectors, which are susceptible to physical tampering and manufacturing defects. This could compromise the system's integrity and performance. Physical tampering can lead to altered quantum states, affecting the accuracy of the computations (Das, Chatterjee and Ghosh, 2023). Manufacturing defects, which are often hard to detect, can introduce unforeseen errors in quantum calculations (Saki et al., 2021). Moreover, the sophistication of these systems could make them vulnerable to side-channel attacks, where an attacker could potentially derive

information from the physical properties of the system (e.g. power consumption, electromagnetic emissions, etc.) (Saki, Topaloglu and Ghosh, 2022). The global supply chain for these specialized components also presents risks (Ghosh, Upadhyay and Saki, 2023), as reliance on external suppliers can introduce vulnerabilities and the possibility of tampering during the manufacturing and distribution processes.

3.2 Software

On the software side, the complexity of the software stack in TI quantum computers presents its own set of challenges. Software that controls quantum computations, manages qubit states, and interfaces with classical computing systems needs regular updates and maintenance. These update and maintenance processes can introduce new vulnerabilities or exacerbate existing ones. Third-party software integration, which is often necessary for specific computational tasks or to enhance system functionality, adds another layer of risk (Das, Chatterjee and Ghosh, 2023). These third-party applications might not always adhere to the stringent security standards required for QC systems which can potentially open backdoors or cause other security gaps (Gachnang et al., 2022). Furthermore, during software updates and maintenance, the system might temporarily have reduced security measures, making it more vulnerable to cyber-attacks. Ensuring the security of software in TIQC involves rigorous testing and validation, constant monitoring for anomalies, and a robust framework for integrating and securing third-party applications (Phalak et al., 2021). Addressing these vulnerabilities is vital for maintaining the integrity and reliability of TIQC systems, especially as they merge into critical infrastructure and high-stakes computing applications.

Table 1: Overview of the Various Security and Privacy Issues in the Quantum Computing Stack (Herman and Friedson, 2018)

Layer of the Quantum Stack	Threat Model
Hardware-level	Input/Output Tampering Crosstalk-induced Fault Injection Readout Sensing Power Side-channel Attacks
Compilation-level	Shuttle-induced Fault Injection Intellectual Property Infringement Input/Output Tampering
Cloud-level	Scheduler Attacks IP Infringement
Application-level	Misclassification Protracted Convergence

4. Cybersecurity Framework for Trapped Ion Quantum Computing

4.1 Framework Pillars

A robust cybersecurity framework for trapped ion quantum computing should be grounded in several foundational pillars: risk assessment, threat modeling, and prevention and mitigation strategies. Each of these pillars plays a crucial role in ensuring the security and integrity of TIQC systems. The pillars and their applications (non-exhaustive) can be seen in Table 2 and the framework is shown in Figure 1.

Figure 1: Trapped Ion Quantum Computing Framework, inspired by (page 3 in document, page 8 of the overall pdf): (NIST CSWP 29, 2024)

Table 2: Trapped Ion Quantum Computing Pillars with Associated Applications

TIQC Framework Pillars	Applications
Risk Assessment	Vetting Component Suppliers Asset-Based Assessment
Threat Modeling	Surveillance Technologies Intrusion Detection Systems Hardware Checks Employee Background Checks
Prevention and Mitigation	Secure Boot Processes Hardware Attestation Methods Encryption Methods Secure Logistics Protocols Employee Access Controls Employee Training Programs Physically Unclonable Functions (Saki *et al.*, 2021) Dummy Gate Obfuscation (Das, Chatterjee and Ghosh, 2023)

4.1.1 Risk Assessment

Risk assessment involves a comprehensive evaluation of the TIQC system to identify potential security vulnerabilities, both in hardware and software. It includes identifying and prioritizing assets within the TIQC system then assessing the potential impact of their compromise on the overall security posture. The potential impact on the security posture should be based upon the criticality of the compromised asset, the likelihood of the threat, and the current capabilities of attackers (U.S. Department of Education, 2003). The analysis of risks from physical tampering, cyber-attacks, manufacturing defects, and supply chain vulnerabilities must be dynamic and continuously updated to account for evolving threats and technological advancements.

4.1.2 Threat Modeling

In this stage, potential threats specific to TIQC are identified and analyzed. This involves understanding how an attacker might exploit hardware and software vulnerabilities and how they might manipulate or intercept third-party components during transport. For classical computing components, the STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege) has been widely used as a threat modelling methodology as it helps to identify potential threats by examining how attackers might exploit vulnerabilities in various computer components (Conklin, no date). However, since models such as STRIDE were developed focusing on classical systems, their applicability to TIQC systems may be limited due to the unique characteristics and architecture of quantum computers.

4.1.3 Prevention & Mitigation Strategies

Based on the previous stages, specific strategies are formulated to protect all components of TIQC.

4.2 Application to Trapped Ion Quantum Computing

When applying this framework to TIQC, particular attention should be given to the following subsections.

4.2.1 Hardware/Software Security

The user should implement security protocols that are specifically tailored to the unique architecture of TIQC systems. This includes securing the quantum processing units, laser systems, electrode control systems, classical control systems, and the interface between them. The user should install advanced surveillance technologies, intrusion detection systems, and provide regular hardware checks (Phalak et al., 2021). This would alert administrators to any physical or digital interference with the quantum hardware, helping to detect tampering and unauthorized access to QC facilities (Das, Chatterjee and Ghosh, 2023). Additionally, secure boot processes and hardware attestation methods could be implemented. This would verify that the quantum computer starts with a trusted software state and ensures that the integrity of the hardware components has not been compromised. Implementing robust encryption methods is also an integral part of this framework, as it would protect the data at rest and in transit.

4.2.2 Supply Chain Integrity Protocols

Ensuring the security and authenticity of third-party components and software is imperative. This involves vetting the suppliers vigorously, verifying the source and origins of components, and ensuring they meet rigorous security standards (Saki, Topaloglu and Ghosh, 2022). Additionally, the logistics of transporting sensitive quantum components require special attention. Tamperproof or tamper-evident packaging (Herman and Friedson, 2018), fault-tolerant designs (Hassija et al., 2020), continuous monitoring during transit, hardware verification methods (Hsia, 2020), and secure storage facilities are essential to protect these components from physical interference and espionage.

4.2.3 Best Practices for Secure Operations

This encompasses a range of practices, from providing physical security of QC facilities to implementing strict access controls and network security protocols. The user should manage personnel and insider threats. This can be accomplished by conducting thorough background checks on employees and implementing strict access controls (Saki et al., 2021). Regular training and awareness programs for employees also foster a culture of security, further preventing the TIQC systems from insider threats (Phalak et al., 2021).

5. Future Outlook & Conclusion

As we gaze into the future of quantum computing, it is evident that the landscape is rapidly evolving, which presents extraordinary capabilities and new challenges. The progression of quantum technologies, particularly trapped ions, will likely unveil many vulnerabilities that are currently unforeseen. This emphasizes the need for a proactive and anticipatory approach to security through adaptive frameworks. Cyber attackers have the advantage of abundant time and creativity, meaning security needs to be as flexible and dynamic as the attackers. The framework for cybersecurity in the quantum realm should include continuous risk assessment, advanced threat detection, and rapid response mechanisms. Quantum computing offers tremendous computational power to transform the world, but to fully realize its potential, security measures are imperative to ensure that quantum computing remains a secure and reliable asset for the advancement of society.

References

Bruzewicz, C.D. *et al.* (2019) 'Trapped-Ion Quantum Computing: Progress and Challenges', *Applied Physics Reviews*, 6(2), p. 021314. Available at: https://doi.org/10.1063/1.5088164.

Conklin, L. (no date) *Threat Modeling Process*, *OWASP*. Available at: https://owasp.org/www-community/Threat_Modeling_Process#stride (Accessed: 18 April 2024).

Das, S., Chatterjee, A. and Ghosh, S. (2023) 'A First Order Survey of Quantum Supply Dynamics and Threat Landscapes'. arXiv. Available at: http://arxiv.org/abs/2308.09772 (Accessed: 1 November 2023).

Gachnang, P. *et al.* (2022) 'Quantum Computing in Supply Chain Management State of the Art and Research Directions', *Asian Journal of Logistics Management*, 1(1), pp. 57–73. Available at: https://doi.org/10.14710/ajlm.2022.14325.

Get to Know Honeywells Latest Quantum Computer System Model H1 (no date). Available at: https://www.honeywell.com/us/en/news/2020/10/get-to-know-honeywell-s-latest-quantum-computer-system-model-h1 (Accessed: 10 December 2023).

Ghosh, S., Upadhyay, S. and Saki, A.A. (2023) 'A Primer on Security of Quantum Computing'. arXiv. Available at: http://arxiv.org/abs/2305.02505 (Accessed: 1 November 2023).

Hassija, V. *et al.* (2020) 'Present landscape of quantum computing', *IET Quantum Communication*, 1(2), pp. 42–48. Available at: https://doi.org/10.1049/iet-qtc.2020.0027.

Herman, A. and Friedson, I. (2018) 'Quantum Computing: How to Address the National Security Risk', *Hudson Institute* [Preprint]. Available at: https://www.hudson.org/national-security-defense/quantum-computing-how-to-address-the-national-security-risk.

Hsia, L.A. (no date) 'Physically Unclonable Characteristics for Verification of Transmon-Based Quantum Computers'.

IBM Quantum (no date). Available at: https://www.ibm.com/quantum (Accessed: 10 December 2023).

IonQ | Trapped Ion Quantum Computing (no date) *IonQ*. Available at: https://ionq.com/ (Accessed: 10 December 2023).

Murali, P. *et al.* (2020) 'Architecting Noisy Intermediate-Scale Trapped Ion Quantum Computers', in *2020 ACM/IEEE 47th Annual International Symposium on Computer Architecture (ISCA)*. *2020 ACM/IEEE 47th Annual International Symposium on Computer Architecture (ISCA)*, Valencia, Spain: IEEE, pp. 529–542. Available at: https://doi.org/10.1109/ISCA45697.2020.00051.

NIST CSWP 29 (2024) The NIST Cybersecurity Framework (CSF) 2.0, National Institute for Standards and Technology. Available at: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf (Accessed: 18 April 2024).

Phalak, K. *et al.* (2021) 'Quantum PUF for Security and Trust in Quantum Computing', *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, 11(2), pp. 333–342. Available at: https://doi.org/10.1109/JETCAS.2021.3077024.

Saki, A.A. *et al.* (2021) 'A Survey and Tutorial on Security and Resilience of Quantum Computing', in *2021 IEEE European Test Symposium (ETS)*. *2021 IEEE European Test Symposium (ETS)*, Bruges, Belgium: IEEE, pp. 1–10. Available at: https://doi.org/10.1109/ETS50041.2021.9465397.

Saki, A.A., Topaloglu, R.O. and Ghosh, S. (2022) 'Shuttle-Exploiting Attacks and Their Defenses in Trapped-Ion Quantum Computers', *IEEE Access*, 10, pp. 2686–2699. Available at: https://doi.org/10.1109/ACCESS.2021.3139085.

U.S. Department of Education (2003) 'Handbook for Information Technology Security Risk Assessment Procedures'. U.S. Department of Education. Available at: https://www2.ed.gov/policy/gen/leg/foia/acshbocio7.pdf (Accessed: 18 April 2024).