The Internet of Quantum Things (IoQT) - A New Frontier in Quantum Emulation and Simulation

Ioannis Kefaloukos[1,*,†], Nikolay Tcholtchev[2,3,†], Michail-Alexandros Kourtis[4,†], Giorgos Oikonomakis[4,†], Emmanouil Eleftherios Rompogiannakis[1,†] and Evangelos Markakis[1,†]

[1]*Hellenic Mediterranean University, Crete, Greece*
[2]*Fraunhofer FOKUS, Berlin, Germany*
[3]*RheinMain University of Applied Sciences, Wiesbaden, Germany*
[4]*National Center of Scientific Research "Demokritos", Greece*

Abstract

In this paper we introduce the concept of the Internet of Quantum Things (IoQT), a distributed quantum development and testing playground that creates a collaborative environment for next-generation quantum developers, connecting quantum simulators and small-qubit devices across secure distributed nodes. Thus, IoQT would provide a cross-quantum programming environment compatible with languages like Qiskit and Eclipse Qrisp enabling IoQT developers to build, test, and validate quantum applications across diverse hardware configurations, while adhering to stringent cybersecurity standards. The IoQT environment envisions quantum-safe encryption protocols, secure hardware compilers, and continuous security monitoring to address quantum-specific cybersecurity challenges. Through the simulation/emulation of realistic, geographically distributed quantum environments, IoQT will be prepared to offer a comprehensive testing ground for quantum applications, thus enabling continuous integration and delivery (CI/CD) with automated security checks. This virtualized framework will empower developers to enhance the security and resilience of quantum applications before transitioning to physical quantum hardware, ensuring that vulnerabilities and quality issues are identified and mitigated early in the development lifecycle. Ultimately, as a secure virtual testing environment, IoQT will support a variety of different stakeholders, including developers, researchers, and industry. The work is in the scope of Project: PQ-REACT (No. 101119547) and Eraclito of the serics foundation.

Keywords

Internet of Quantum Things (IoQT), Distributed Quantum Computing, Quantum Simulation, Quantum Key Distribution (QKD), Self-Healing Systems, Anomaly Detection, Secure Quantum Networks, Quantum Application Development,

1. Introduction

The Internet of Quantum Things (IoQT) represents a groundbreaking shift in how quantum emulating devices can interact, communicate, and collaborate across distributed networks. As quantum computing capabilities grow, so does the need for a quantum-specific communication and computing infrastructure that can handle the unique requirements of quantum algorithms. Furthermore, despite the continuous announcements of breakthroughs, real quantum computing on physical Quantum Processing Units (QPUs) is still far from being competitive. This also hampers the development and experimentation with new quantum algorithms, since the current quantum state-simulators can show potential advantages only on a limited scale, basically making it difficult to extensively research and evaluate approaches that could potentially bring benefits on real QPUs. By introducing IoQT, we aim to provide the means for

Joint National Conference on Cybersecurity (ITASEC & SERICS 2025), February 03-8, 2025, Bologna, IT
*Corresponding author.
†These authors contributed equally.
g.kefaloukos@pasiphae.eu (I. Kefaloukos); nikolay.tcholtchev@fokus.fraunhofer.de (N. Tcholtchev); akis.kourtis@iit.demokritos.gr (M. Kourtis); goikonomakis@iit.demokritos.gr (G. Oikonomakis); m.rompogiannakis@pasiphae.eu (E. E. Rompogiannakis); markakis@pasiphae.eu (E. Markakis)
0000-0002-1041-9206 (I. Kefaloukos); 00000-0001-6821-4417 (N. Tcholtchev); 0000-0002-8356-114X (M. Kourtis); 0009-0000-2060-7326 (E. E. Rompogiannakis); 0000-0003-0959-598X (E. Markakis)

distributed quantum simulations - thereby (small) IoT devices are meant to emulate single qubits on their classical processors and realize multi-qubit gates thereby utilizing the underlying (tele-)communication network, in order to facilitate the exchange between the emulated qubits. This paper aims to define the IoQT, outline its potential architecture, and identify the unique challenges and solutions associated with this new quantum simulation/emulation paradigm. The paper is structured as follows: Section 1 introduces the concept of IoQT, its envisioned capabilities, and its importance in addressing challenges in quantum simulation and emulation. Section 2 provides a detailed background, exploring the state-of-the-art in quantum networking, IoT security, and distributed computing. Section 3 introduces the IoQT architecture and demonstrates its capabilities through a practical use case. Section 4 highlights the unique challenges and corresponding solutions associated with the IoQT framework, while Section 5 delves into the potential applications and broader impact. Section 6 outlines the implementation and evaluation metrics, Section 7 presents Eclipse Qrisp as a possible Front-End, and finally, Section 8 concludes the paper, summarizing the contributions and future prospects of the IoQT framework.

2. Background

This section investigates the state of the art in quantum networking, secure IoT, and distributed computing systems. To achieve secure data transmission, quantum networks leverage protocols such as Quantum Key Distribution (QKD). However, scaling these networks for internet-like structures remains an open challenge [1], whereas current efforts are focusing on connecting isolated quantum nodes with a limited number of qubits, hence lacking the robustness and scalability needed for widespread adoption. Several other research endeavours and experimental demonstrations involve entangled photon distribution and quantum repeaters showcased that while they have made significant advancements still face technological limitations (e.g., photon loss over long distances, imperfections in photon sources, sensitivity of entanglement to environmental noise, need for high-fidelity entanglement operations, long-lived quantum memories, and robust error correction mechanisms[2, 3, 4, 5]). Additionally, IoT systems have undergone extensive research, yet traditional IoT security protocols are inadequate to tackle and emulate multi-qubit systems [6, 7]. Hence, enhancing IoT security with quantum-resilient encryption [8] and distributed simulation frameworks is still an open issue [9]. Recent advancements in blockchain-based IoT security [10] and AI-enhanced intrusion detection [11], offer promising pathways, if they adapt to handle quantum-specific data. Continuing, research in distributed quantum computing primarily addresses synchronization and coherence across quantum nodes. Techniques such as quantum teleportation [12] and error correction codes have been proposed to maintain coherence in distributed settings [13]. In addition, ongoing studies highlight the role of hybrid quantum-classical systems in supporting efficient quantum simulations [14]. These systems leverage classical nodes to manage non-quantum tasks while coordinating quantum operations, ensuring optimal performance in distributed environments. IoQT aims to build upon these advancements by introducing a scalable, secure, and real-time communication framework for distributed quantum simulations, integrating synchronization protocols and robust error correction mechanisms to address the unique challenges of distributed quantum computing.

3. IoQT Architecture and Use Case

In this section we will delve within the proposed IoQT Architecture and a use case

3.1. IoQT Architecture

The IoQT architecture is built to accommodate distributed quantum computing simulation, emphasizing security, scalability, and efficient communication. Figure 1 illustrates the overall proposed high-level architecture of the platform. Thereby, the stakeholders can be seen interacting with the Quantum Computing Infrastructure, which could include QPUs. However, it could also make a virtual reroute

to the external distributed overlay of Internet of Quantum Things, in which distributed small devices (e.g. sensor nodes) - but also traditional PCs, laptops and servers - are used to simulate/emulate single qubits and enable the large scale distributed simulation/emulation of quantum processing over the Internet. All the "Quantum Things" are basically accessed over a middleware overlay providing secure communication in addition to intrinsic self-healing and self-organisation mechanisms. The qubit simulation can be geographically highly distributed and can also accommodate voluntarily provided and integrated devices, which belong to community members. The proposed IoQT framework includes the following components:

Quantum Node Emulator: Each node in the IoQT network functions as a Quantum Node Emulator. This component is designed to emulate quantum devices (such as qubits) on classical hardware, hence is capable of performing basic quantum operations, including single-qubit gates and multi-qubit gate operations (e.g., CNOT gates), which are essential for simulating quantum algorithms. In more detail the quantum node emulator includes:

- **Emulation Techniques:** The emulation process involves quantum circuit models that simulate qubit states and their evolution over time. Classical processors handle the emulation of quantum behaviour, with specific algorithms tailored to approximate quantum interference and superposition.
- **Real-time Synchronization:** To maintain coherence across the quantum network, the emulators use synchronization protocols to ensure that the operations performed by different nodes stay aligned, mitigating any discrepancies that could arise from network latencies or computational errors.
- **Virtual Quantum Environment:** The Quantum Node Emulator can integrate with other classical systems (e.g., for logistical optimization) to simulate quantum state exchanges across various geographically distributed nodes.

Secure Communication Layer: This layer is pivotal for maintaining the integrity and confidentiality of quantum information exchanged between nodes, utilising quantum-safe protocols designed specifically to prevent quantum attacks. In more detail, the secure communication layer could include:

- **Quantum Key Distribution (QKD):** QKD ensures that any communication of quantum states is encrypted with quantum-resilient cryptography. It allows for secure key exchange even in the presence of quantum-powered adversaries.
- **Post-Quantum Encryption (PQE):** For classical data exchanges, IoQT uses PQE algorithms that remain secure in the face of quantum computing advancements. This guarantees that sensitive data and the results of quantum simulations are protected.
- **Secure Channel Management:** The layer ensures that communication links between nodes are protected from eavesdropping and tampering, maintaining the confidentiality of the quantum data in transit.

Self-Healing and Anomaly Detection Module: Using AI-driven anomaly detection, this module monitors the communication (resulting from the quantum simulation) in real time, identifying any irregularities or potential security breaches and automatically triggering corrective actions. This module includes:

- **Real-time Monitoring:** Using machine learning algorithms, the system scans for irregularities in data transmission, quantum state degradation, or faulty qubit interactions that may signal potential security breaches or operational failure.
- **Automatic Fault Correction:** Upon detecting an anomaly, the system automatically triggers corrective actions such as re-synchronizing quantum states, rebooting nodes, or shifting quantum operations to backup nodes to maintain system stability and prevent cascading failures.
- **Intrusion Detection Systems (IDS):** The anomaly detection module also functions as an advanced intrusion detection system (IDS), capable of identifying unusual behaviors indicative of cyberattacks. This allows the system to isolate compromised components quickly.

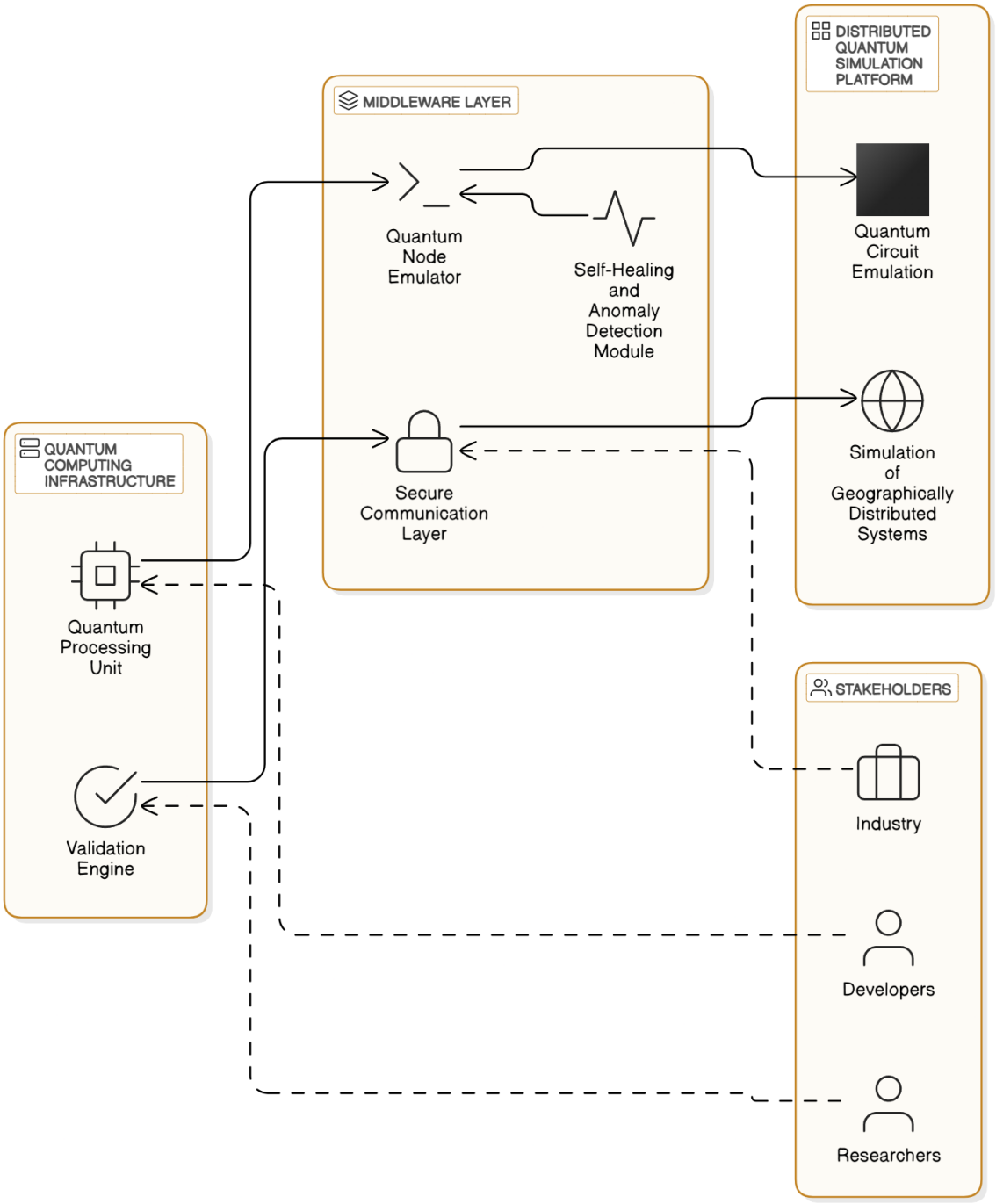

Figure 1: IoQT Framework High-Level Architecture.

Distributed Quantum Simulation Platform: A core feature of IoQT is its ability to simulate quantum networks or multi-qubit gates across multiple quantum emulating/simulating nodes, providing an environment to test quantum algorithms, applications, and their interactions in close-to real-world scenarios. In more detail, this module contains the following:

- **Quantum State Simulation:** The platform simulates multi-qubit gates across multiple quantum emulating nodes. Each node can independently simulate qubits, while also coordinating with neighboring nodes to ensure consistency across the quantum network.
- **Scalable Architecture:** The platform can scale to accommodate additional nodes, allowing for

the simulation of larger quantum systems and their associated operations. The distributed nature of the platform ensures that the computational load is shared across multiple devices, enabling large-scale simulations that are beyond the capability of a single quantum processor.

- **Error Resilience and Fault Tolerance:** The platform integrates quantum error correction techniques such as surface codes and concatenated codes, enabling it to handle common quantum computing issues like decoherence, gate fidelity loss, and qubit leakage.
- **Quantum Cloud Integration:** The platform is designed to interface seamlessly with existing quantum cloud services to allow real-world quantum applications to be tested on both virtual and physical hardware.

Each component is designed to support the specific needs of quantum applications/services/algorithms, facilitating secure quantum computation, efficient data transmission, and continuous network integrity checks.

3.2. IoQT Use Case

To demonstrate the capabilities of the IoQT platform, we will examine a use case where a distributed quantum algorithm is developed to optimize a global supply chain network.

The IoQT platform offers a comprehensive solution for the development and optimization of quantum applications within intricate, distributed systems. To demonstrate the capabilities of the IoQT platform, in this subsection, we will examine a use case where a distributed quantum algorithm is developed to optimize a global supply chain network. The process begins with the configuration of a virtual quantum environment within the IoQT framework. This environment consists of quantum nodes, each emulating quantum hardware at key supply chain locations, such as warehouses, distribution hubs, and transport points. These nodes are interconnected to mirror real-world operational constraints, such as communication delays and resource limitations.

The development phase involves the implementation of quantum algorithms, utilizing for example the Eclipse Qrisp [17] with its corresponding arithmetic capabilities [15] and abstractions [16], thus **addressing combinatorial optimization problems**. For instance, the algorithm may focus on minimizing logistics costs, reduce delivery times, and streamline resource allocation across the network. The Quantum Node Emulator will ensure accurate simulations of quantum states and multi-qubit gate operations across the distributed nodes, while accounting for qubit interactions and gate execution latencies.

Once the algorithm is formulated, the Distributed Quantum Simulation Platform facilitates its execution, **simulating quantum state exchanges** between geographically distributed nodes. The Context Awareness Layer will continuously adapt the simulation parameters, dynamically addressing environmental variations, such as increased error rates or network delays. This capability ensures that the performance of the quantum application remains robust under varying conditions.

To tackle the security challenges during development and executing, the Secure Communication Layer will enforce **quantum-safe encryption** for all transmitted data, hence ensuring that the confidentiality and integrity of quantum information exchanged between nodes. Additionally, the Self-Healing and Anomaly Detection (AD) module will monitor the simulated environment, detecting anomalies such as communication faults or unexpected behaviours. Corrective actions will trigger automatically, thus safeguarding the stability of the quantum system.

Following executing, the Oracle interface will provide **insights into the performance** of the quantum algorithm. Metrics such as circuit depth, execution time, error rates, and qubit synchronization will be analysed, identifying bottlenecks and opportunities for optimization (e.g., inefficiencies in communication between nodes may necessitate adjustments to reduce computational overhead and enhance performance).

The final step includes the validation and deployment of the aforementioned **refined** quantum algorithm. The CI/CD pipeline will ensure seamless validation through automated testing, hence enabling the application to be transferred to physical quantum hardware or hybrid quantum-classical

systems. This continuous integration approach ensures that updates and refinements are rigorously tested before the deployment, guaranteeing operational stability.

4. Key Challenges and Solutions

Identifying and addressing the unique technical challenges in establishing the IoQT is crucial for its success. Hence, a breakdown of the challenges and the proposed solutions can be seen below:

Synchronization of simulated Quantum States: The exchange of information about simulated quantum states between the involved IoQT devices depends highly on the dynamics and capacity of the underlying communication network. IoQT will address this through advanced synchronization protocols that reduce the communication overhead in a distributed quantum simulating/emulating system.

Scalability of network communication between IoQT devices: IoQT should scale, thereby maintaining secure and reliable communication between the involved quantum emulating/simulating devices. The use of distributed quantum simulation and high-performance connectivity enhances scalability in addition to allowing extensive testing and monitoring across networked quantum emulating devices.

Quantum-Specific Security: IoQT incorporates quantum-resilient encryption and real-time intrusion detection systems (IDS) tailored to the specific quantum simulating/emulting data, ensuring that all communications and computations remain secure.

5. Potential Applications and Impact

The IoQT has the potential to transform several key sectors by introducing secure and scalable quantum simulation functionalities described here:

Collaborative Quantum Computing: By enabling multiple quantum simulating/emulating systems to work together, IoQT can support collaborative quantum computing applications, including complex simulations for drug discovery, climate modeling, and materials science.

Quantum-Enabled IoT for Critical Infrastructure: IoQT can be used to secure critical infrastructures, such as energy grids and transportation networks, where distributed quantum computing and real-time security monitoring are essential.

6. Implementation and Evaluation

This section will delve into the details of the proposed implementation strategy for the IoQT, along with key metrics for its evaluation.

Theoretical Model: At the beginning, we plan to specify the theoretical module of a Distributed Quantum Cellular Automaton (DQCA), which will describe the functioning and possible states of a set of theoretical finite automata that could calculate the functions implemented by quantum circuits.

Implementation Phases: IoQT implementation will proceed in stages, starting with simulation-based testing of core components (e.g., Secure Communication Layer, Anomaly Detection Module), followed by gradual integration of quantum nodes in real environments. Thereby, we plan to follow and implement in reality the computational principles of the DQCA mentioned above.

User interfaces: In this step we plan to integrate the IoQT infrastructure with established user interfaces in terms of programming frameworks. Typical examples for such user interfaces are provided by Qiskit and Eclipse Qrisp.

Evaluation Metrics: The success of IoQT will be measured through key performance indicators (KPIs) such as circuit depth of the executed quantum circuits, error rates, network latency, quantum state synchronization time, implemented user level quantum algorithms (Grover, Shor, QUBO, QAOA, VQE, etc.), security breach detection rates, and system uptime under varying network loads.

Expected Outcomes: The pilot aims to validate IoQT's potential for secure, large-scale distributed quantum simulation and lay the groundwork for future quantum-enhanced architectures.

7. Eclipse Qrisp as a possible Front-End

We perceive Eclipse Qrisp [17] as a possible front-end towards the end users utilizing IoQT for executing their hybrid-quantum programs. Eclipse Qrisp [18] is a Python embedded domain specific language (i.e. eDSL) that allows implementing high-level quantum program structures together with classical and GPU-based algorithms. In contrast to other existing quantum languages, Eclipse Qrisp aims at providing a higher level of abstraction thereby enabling the programming with variables, data types, functions, if-then-else conditions, iterations and other high- level language constructs instead of sticking to directly addressing qubits and gates as done in the majority of existing frameworks.

```
from qrisp import QuantumFloat
n = 6
a = QuantumFloat(n)
b = QuantumFloat(n)
a[:] = 3
b[:] = 4
res = a*b

print(res)

#Yields: {12: 1.0}
```

The above code listing gives a glimpse into the level of abstraction enabled by Qrisp. We see the implementation of a simple float multiplication, which is abstracted on the level of variables and overloaded operations. The QuantumFloat object hides the explicit handling and organization of the qubits and structures required to realize a floating point number, while the multiplication is executed on the quantum computer/simulator based on the structure of the float numbers. The final result is provided by the product of the two floats with its assigned probability. We can see that the code is independent from the underlying hardware architecture, i.e. the specific qubits, gates and interconnections. Hence, the complexity of translating this code to the hardware specific features is delegated to the underlying compiler (and transpiler), which would also be enabled to translate the code to the specific interfaces of IoQT in the future.

8. Conclusions

IoQT represents a transformative step towards democratizing quantum computing by offering a secure and scalable simulation environment. Its distributed architecture addresses critical challenges in quantum state synchronization, scalability, and security, laying the groundwork for a collaborative quantum ecosystem. By enabling developers to validate quantum applications in realistic conditions, IoQT accelerates innovation while ensuring the security and reliability of future quantum technologies. Furthermore, IoQT paves the way for interdisciplinary collaboration, bridging gaps between quantum computing, IoT, and distributed systems. Its potential to enhance critical infrastructure resilience and drive breakthroughs in scientific domains positions it as a cornerstone in the future of quantum technology. As quantum computing continues to evolve, platforms like IoQT will play a pivotal role in transitioning theoretical advancements into practical, real-world solutions. The successful implementation of IoQT could serve as a template for global initiatives in quantum research and development, fostering an era of secure, efficient, and accessible quantum technologies. The platform's potential applications in critical infrastructure and collaborative computing further highlight its significance in advancing quantum research and development.

Declaration on Generative AI

During the preparation of this work, the authors used eraser.io for figure 1 in order to: Generate images. After using these tool(s)/service(s), the author(s) reviewed and edited the content as needed and take(s) full responsibility for the publication's content.

References

[1] S.-H. Wei, et al., Towards real-world quantum networks: A review, Laser and Photonics Reviews 16 (2022). doi:10.1002/lpor.202100219.

[2] K. Azuma, S. E. Economou, D. Elkouss, P. Hilaire, L. Jiang, H.-K. Lo, I. Tzitrin, Quantum repeaters: From quantum networks to the quantum internet, Reviews of Modern Physics 95 (2022). doi:10.1103/RevModPhys.95.045006.

[3] K. Goodenough, D. Elkouss, S. Wehner, Optimizing repeater schemes for the quantum internet, Physical Review A 103 (2021) 032610. doi:10.1103/PHYSREVA.103.032610.

[4] C. Schimpf, M. Reindl, F. Basso Basset, K. D. Jöns, R. Trotta, A. Rastelli, Quantum dots as potential sources of strongly entangled photons: Perspectives and challenges for applications in quantum networks, Applied Physics Letters 118 (2021). doi:10.1063/5.0038729.

[5] S. Simmons, Scalable fault-tolerant quantum technologies with silicon color centers, PRX Quantum 5 (2024) 010102. doi:10.1103/PRXQUANTUM.5.010102.

[6] S. Cherbal, A. Zier, S. Hebal, L. Louail, B. Annane, Security in internet of things: A review on approaches based on blockchain, machine learning, cryptography, and quantum computing, Journal of Supercomputing 80 (2024) 3738–3816. doi:10.1007/S11227-023-05616-2.

[7] E. Ebrahimpour, S. Babaie, Authentication in internet of things, protocols, attacks, and open issues: A systematic literature review, International Journal of Information Security 23 (2024) 1583–1602. doi:10.1007/S10207-023-00806-8.

[8] M. García-Cid, M.-A. Kourtis, D. Domingo, N. Tcholtchev, E. K. Markakis, M. Niemiec, V. Martín, D. López, M. Gagliard, J. González, M. García, G. Comande, N. Stoianov, PQ-REACT: Post quantum cryptography framework for energy aware contexts, in: Proceedings of the 19th International Conference on Availability, Reliability and Security (ARES 2024), 2024. URL: https://dl.acm.org/doi/10.1145/3664476.3670868. doi:10.1145/3664476.3670868.

[9] T. Liu, G. Ramachandran, R. Jurdak, Post-quantum cryptography for internet of things: A survey on performance and optimization, 2024. URL: https://arxiv.org/abs/2401.17538v1. arXiv:2401.17538v1.

[10] O. Alkadi, N. Moustafa, B. Turnbull, K. K. R. Choo, A deep blockchain framework-enabled collaborative intrusion detection for protecting iot and cloud networks, IEEE Internet of Things Journal 8 (2021) 9463–9472. doi:10.1109/JIOT.2020.2996590.

[11] M. Kalinin, V. Krundyshev, Security intrusion detection using quantum machine learning techniques, Journal of Computer Virology and Hacking Techniques 19 (2023) 125–136. doi:10.1007/S11416-022-00435-0.

[12] C. Ryan-Anderson, N. C. Brown, C. H. Baldwin, J. M. Dreiling, et al., High-fidelity and fault-tolerant teleportation of a logical qubit using transversal gates and lattice surgery on a trapped-ion quantum computer, 2024. doi:10.1126/science.adp6016.

[13] D. S. Wang, Y. D. Liu, Y. J. Wang, S. Luo, Quantum resource theory of coding for error correction, Physical Review A 110 (2024) 032413. doi:10.1103/PHYSREVA.110.032413.

[14] T. Lubinski, C. Granade, A. Anderson, A. Geller, M. Roetteler, A. Petrenko, B. Heim, Advancing hybrid quantum–classical computation with real-time execution, Frontiers in Physics 10 (2022) 940293. doi:10.3389/FPHY.2022.940293.

[15] R. Seidel, C. Becker, S. Bock, N. Tcholtchev, I. Gheorghe-Pop, M. Hauswirth, Automatic generation of grover quantum oracles for arbitrary data structures, Quantum Science and Technology 8 (2023) 025003.

[16] R. Seidel, N. Tcholtchev, S. Bock, M. Hauswirth, Uncomputation in the qrisp high-level quantum programming framework, in: M. Kutrib, U. Meyer (Eds.), Reversible Computation. RC 2023, volume 13960 of *Lecture Notes in Computer Science*, Springer, Cham, 2023. doi:10.1007/978-3-031-38100-3_11.

[17] R. Seidel, S. Bock, R. Zander, M. Petrič, N. Steinmann, N. Tcholtchev, M. Hauswirth, Qrisp: A framework for compilable high-level programming of gate-based quantum computers, 2024. URL: https://arxiv.org/abs/2406.14792. arXiv:2406.14792.

[18] E. Qrisp, Eclipse qrisp: A framework for high-level quantum programming, 2024. Available at: https://qrisp.eu (Accessed: 14.01.2024).