e-ISSN: 2582-5208

International Research Journal of Modernization in Engineering Technology and Science

(Peer-Reviewed, Open Access, Fully Refereed International Journal)

Volume:06/Issue:07/July-2024 Impact Factor- 7.868 www.irjmets.com

THE FUTURE OF CYBERSECURITY IN THE AGE OF QUANTUM COMPUTERS

Roshani Sonone[*1], **Dr. A.A. Bardekar**[*2]

[*1]Student, Department Of Computer Science And Engineering, Sipna College Of Engineering And Technology, Amravati Maharashtra, India.

[*2]Professor, Department Of Computer Science And Engineering, Sipna College Of Engineering And Technology, Amravati Maharashtra, India.

ABSTRACT

The first shocker of the year arrived six months earlier, when one of the four post-quantum cryptography (PQC) algorithms selected by NIST (National Institute of Standards and Technology) was taken down. Unfortunately, both failed PQC algorithms are commercially available. The second shocker came in the first week of August 2022, as another NIST finalist was cracked by a team from Belgium in just 62 minutes using a standard laptop, earning them a USD 50,000 bounty from Microsoft. With 80 out of 82 PQC candidates failing the NIST standardization process, the future of the remaining two is in question, jeopardizing the 5-year NIST exercise to establish a quantum-safe encryption standard.

Meanwhile, the looming quantum threat persists. This paper advocates stepping back to review the root causes of the problem. While current computer security heavily relies on cryptography, it can transcend encryption alone. The paper explores an encryption-agnostic approach—Zerovulnerability computing (ZVC)—which secures computers by eliminating all third-party permissions, a major source of vulnerabilities. ZVC simplifies the complex architecture of legacy computers, opting instead for a minimalist, energy-efficient solid-state software on a chip (3SoC) that may offer resistance to malware and quantum threats.

Keywords: Quantum Computers; Quantum Threat; Cybersecurity; Computer Vulnerabilities; PQC; Computer Architecture; NIST; Hacking; Solid State.

I. INTRODUCTION

Quantum computing, initially envisioned by Richard Feynman and Yuri Manin over four decades ago [1], has gained substantial momentum in the past decade (Figure 1). The theoretical potential of quantum computers to perform certain computational tasks exponentially faster than classical computers marks a milestone in experimental quantum supremacy [2].

While quantum scientists anticipate the transformative benefits of quantum computing [3], concerns about cybersecurity loom large. With the quantum computing industry projected to reach USD 10.5 trillion by 2025 [5], the threat of quantum-powered cybercrime is becoming increasingly real [6]. Recent quantum attacks on cryptocurrencies have even triggered market crashes [7]. The cybersecurity community is actively addressing the technological implications of quantum computing [8], amidst warnings of a potential quantum apocalypse [9] and comparisons to existential risks posed by artificial intelligence [10].

The imminent quantum threat to legacy computers necessitates proactive measures. Broadly, strategies include: (i) enhancing individual protection of Internet-connected legacy computers against quantum attacks, and (ii) segregating quantum computing activities from mainstream Internet infrastructure.

As outlined in Section 2, current practices primarily focus on safeguarding individual computers using PQC (post-quantum cryptography) algorithms. **However, as detailed in Sections 3 and 4**, this paper advocates for an alternative strategy. Rather than widespread adoption of PQC across the Internet, our approach involves isolating quantum computing activities. This approach recognizes the emerging trend where quantum computing is transitioning towards a subscription-based model known as QaaS (Quantum-as-a-Service), rather than being freely accessible to all.

Section 5 discusses the reasons behind this shift. It is evident that quantum computing is rapidly evolving into a specialized service model catering to high-power computing needs of specific industries. Consequently, subscribers of QaaS are likely to be required to adhere to specific security protocols to access quantum computing resources.

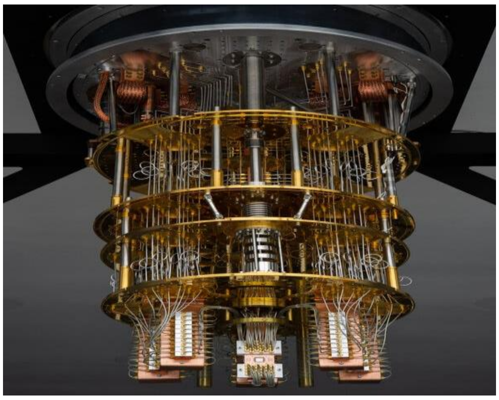


Figure 1. IBM quantum computer.

- There is a growing interest in cloud-based quantum computers.
- Recent advances indicate that Quantum-as-a-Service (QaaS) has become a viable option [11].
- At least six QaaS providers, including Amazon and IBM, have launched platforms allowing scientists, researchers, and developers to build, test, and run quantum computing algorithms [12].
- IBM even offers its QaaS for free [13].
- Subscription to QaaS offerings may require deploying specific security protocols for access.
- This paper draws from a recent report on "zero-vulnerability computing (ZVC)" [14] to examine a pertinent question: Can ZVC's encryption-agnostic approach ensure quantum-safe computing?
- ZVC's encryption-agnostic security protocol holds promise in providing unbreakable end-to-end security for accessing QaaS and segregating it from the broader Internet.
- The QaaS access authentication approach proposed in this paper effectively eliminates the risk of exposing legacy computers to encryption-breaking quantum algorithms, rendering the recent failures of PQC algorithms inconsequential.

This paper presents observational research that compiles empirical data to support the quantum-safe hypothesis regarding the future of cybersecurity. In Section 6, it concludes that, instead of attempting to protect each Internet-connected device individually from quantum attacks, the optimal strategy for addressing the impending quantum threats to the Internet is to regulate QaaS access and segregate all subscription-based quantum computing activities from the mainstream Internet.

II. PROBLEM STATEMENT

In November 2017, 82 candidate algorithms were submitted to the NIST (National Institute of Standards and Technology) for consideration in a public competition to select PQC (post-quantum cryptography) algorithms [15]. This initiative was launched to address the impending security threats from quantum computers, which are projected to become fully functional by 2030 [16].

These quantum systems will have the capability to execute algorithms that can decrypt most of today's asymmetric security protocols, such as RSA or elliptical curve algorithms. Experts recommend that industries prepare for PQC based on the shelf life of data and system lifetime [17].

For instance, according to a McKinsey Digital report (Figure 2), certain data with long shelf lives—such as classified government documents, personal health data, or corporate trade secrets—will remain valuable when the first quantum computers are expected to become available. Any data transferred today on public networks that retain relevance over time are at risk of interception and future decryption by quantum computers.

Examples include long-term life insurance plans or 30-year home mortgage loan contracts, which may already be vulnerable to future quantum threats because they will still be active when quantum computers are commercially viable.

After a rigorous five-year evaluation process, which included three "NIST PQC Standardization Conferences" [18] and extensive deliberations on NIST's PQC forum, four finalists were selected from submissions by the international crypto research community [19].

Earlier this year, New Scientist reported that a post-quantum encryption algorithm (Rainbow), approved by the NIST, could be easily cracked using a standard laptop [20].

More recently, researchers from the Security and Industrial Cryptography group (CSIS) at KU Leuven demonstrated that with a single core of a regular Intel Xeon CPU (2013 release), they successfully cracked the second algorithm (SIKE, short for Supersingular Isogeny Key Encapsulation) among the four encryption algorithms considered to resist decryption by quantum computers [21] [22]. SIKE was developed by a consortium including Amazon, Infosec Global, Microsoft Research, Texas Instruments, and various international universities. The KU Leuven team received a USD 50,000 bounty for their breakthrough, which stunned the quantum computing community.

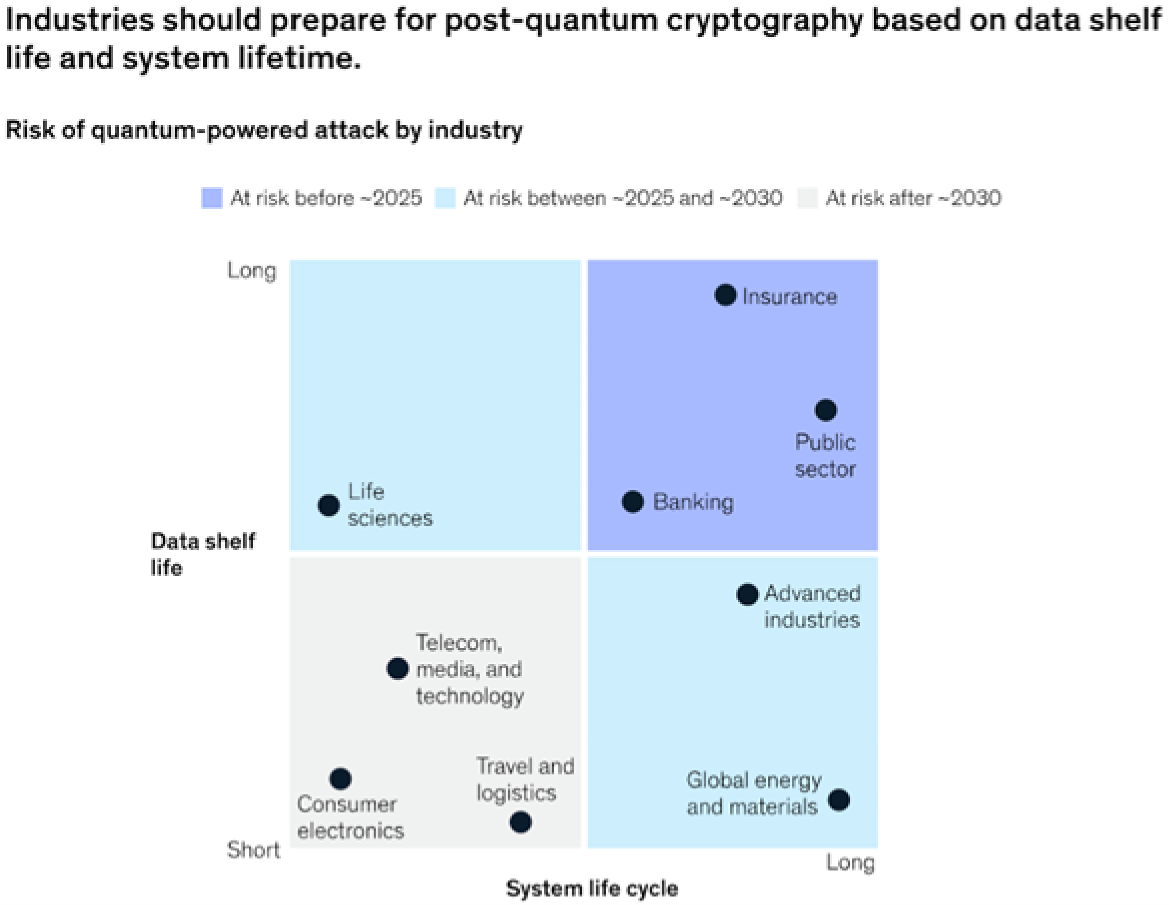


Figure 2. Risk of quantum-powered attack by industry

With two out of the four candidate PQC algorithms that reached the fourth round of NIST validation failing, the future of the remaining two candidates appears uncertain. Despite the fact that actual quantum computers have yet to be realized, the cryptography designed to withstand them is already being tested. If PQC algorithms can be cracked so easily, the future of cybersecurity looks increasingly uncertain.

III. IS THE QUANTUM THREAT UNASSAILABLE?

Since the inception of modern personal computers, cryptography has been pivotal in safeguarding sensitive information by scrambling it to thwart unauthorized access [23]. However, the challenge of physically gating access to computer resources remains daunting, as legacy systems default to granting permissions to all applications, thereby introducing vulnerabilities that necessitate increasingly complex encryption algorithms [24]. With the exponential rise in connected devices, these vulnerabilities have grown substantially [25].

The emphasis of computer security has largely shifted towards cryptography, sidelining the importance of physical access gating. This shift leaves computer security vulnerable to the anticipated computational power of future quantum computers. Hence, it is imperative to reconsider the neglected aspect of security—physical access gating to information.

A recent report on zero-vulnerability computing (ZVC) offers a promising alternative [14]. ZVC represents a new cybersecurity paradigm that is independent of specific encryption methods and is supported by over 30 European partners in the European Commission's Horizon program [26]. Initial experiments with ZVC have led to hypotheses:

- Can ZVC inherently resist quantum threats due to its encryption-agnostic nature?
- Does the layerless architecture of ZVC, akin to the simplicity of solid-state electronics, offer transformative advantages for computing akin to the revolution of solid-state electronics in the 1960s–1970s?

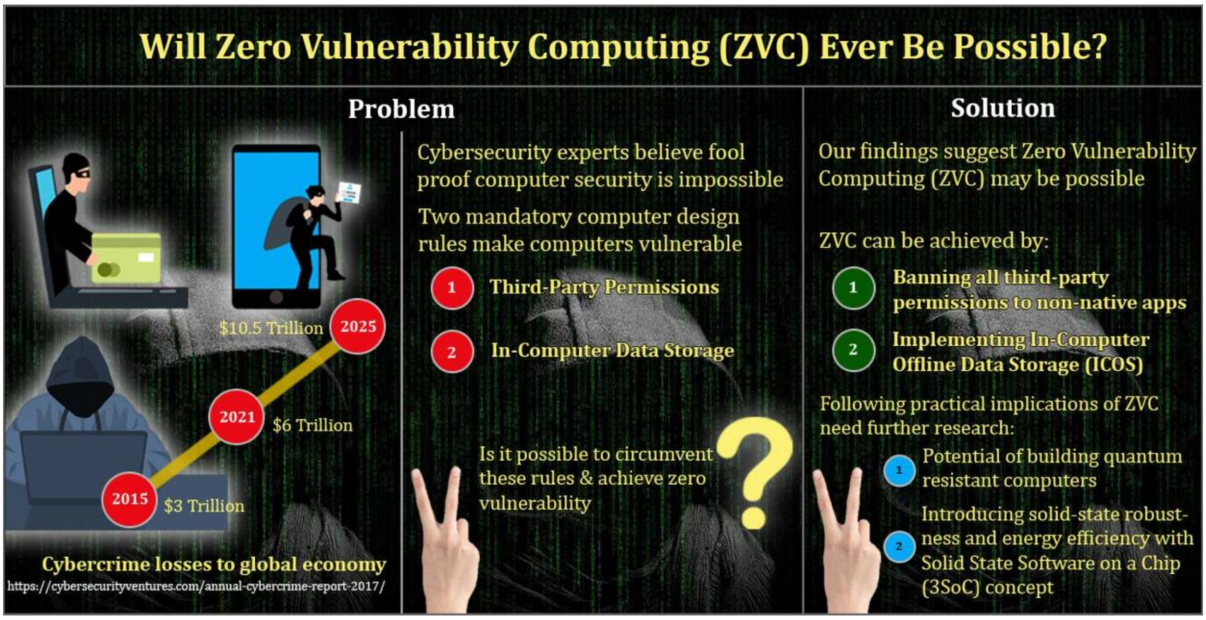
Ongoing research by a European consortium aims to validate these hypotheses and explore the technological foundations supporting them. Such an exploration not only seeks alternative approaches to counter quantum threats but also introduces the potential for a new era of solid-state software on a chip (3SoC) that integrates the reliability and robustness of solid-state electronics into software design [27].

With this objective, a detailed exploration of the components and principles of ZVC is presented herein.

IV. HOW DOES ZVC WORK?

Legacy computers, whether based on the von Neumann architecture [28] or the Harvard architecture [29], cannot function without granting permissions to third-party applications. These permissions inherently introduce vulnerabilities, compounded by the mandatory online status of stored data in connected computers (Figure 3).

Achieving zero vulnerability with existing architectures is considered impossible without significant changes that restrict permissions and access to stored data. Zero Vulnerability Computing (ZVC) addresses this challenge by fundamentally transforming traditional computer architectures to impose stringent restrictions on permissions and data access, as recently defined [14].



Will Zero Vulnerability Computing (ZVC) Ever Be Possible?

Problem

Cybersecurity experts believe fool proof computer security is impossible

Two mandatory computer design rules make computers vulnerable

1 Third-Party Permissions

2 In-Computer Data Storage

Is it possible to circumvent these rules & achieve zero vulnerability

Cybercrime losses to global economy

https://cybersecurityventures.com/annual-cybercrime-report-2017/

Solution

Our findings suggest Zero Vulnerability Computing (ZVC) may be possible

ZVC can be achieved by:

1 Banning all third-party permissions to non-native apps

2 Implementing In-Computer Offline Data Storage (ICOS)

Following practical implications of ZVC need further research:

1 Potential of building quantum resistant computers

2 Introducing solid-state robustness and energy efficiency with Solid State Software on a Chip (3SoC) concept

Figure 3. Zero vulnerability computing (ZVC): A graphical abstract

ZVC is a cybersecurity paradigm proposing a novel computer architecture with a zero-attack surface. It restricts all third-party applications exclusively to a web interface, denying permissions for any non-native program to access computing resources. Additionally, ZVC includes switchable in-computer offline storage, enabling users to secure sensitive data as needed.

Understanding the definition of ZVC leads to two critical considerations

4.1. Encryption-Agnostic Security of ZVC

In traditional computing systems, both hardware and software inherently grant permissions to third-party vendors and developers, enabling a wide array of applications that enhance computer functionality. These permissions, essential for running diverse applications, also introduce vulnerabilities that are frequently exploited by hackers, thereby creating an attack surface that cannot be completely eliminated. Moreover, the necessity of maintaining online connectivity for data accessibility further exposes connected devices to cyber threats. These foundational rules, effective in the pre-Internet era, have proven inadequate in preventing modern cybercrimes, leading experts to conclude that achieving fool-proof cybersecurity is practically impossible.

ZVC addresses these challenges by:

1. **Banning all third-party permissions:** This effectively eliminates the attack surface.
2. **Implementing switchable in-computer offline storage:** This capability resides within the device itself.

For encrypted data to be vulnerable to quantum computers (QCs), they must be discoverable and exposed to quantum cryptographic algorithms. Encrypted data under PKI (private–public-key infrastructure) typically fall into two categories:

- **Device access authentication data**
- **Data stored on the device's memory**

ZVC safeguards against potential quantum attacks in the following ways:

1. **Device access authentication data:** Quantum computers can remotely break current encryption standards, contingent on online accessibility to the victim resource and freedom for unlimited decryption attempts. ZVC's ICOS (in-computer offline storage) module mitigates this by going offline automatically after three unsuccessful attempts, rendering the private data inaccessible to QC algorithms.
2. **Data stored on the device's memory:** If a QC algorithm breaches access authentication, it gains access to all discoverable data. ZVC secures private data on NAND memory behind two security gates, requiring the QC to execute its algorithms locally on the device, akin to typical malware. ZVC prohibits all third-party permissions at the hardware level, preventing the execution of non-native algorithms and recognizing targeted data on the breached device. Once access is breached, the QC cannot transfer codes to run locally due to the absence of third-party permissions. Thus, breaking access encryption becomes futile as further local execution of remote malicious code is impossible, ensuring the security of ZVC-protected data.

ZVC's methodology secures native data by setting up two gates that must be successfully passed before data becomes accessible, as illustrated in Figure 4.

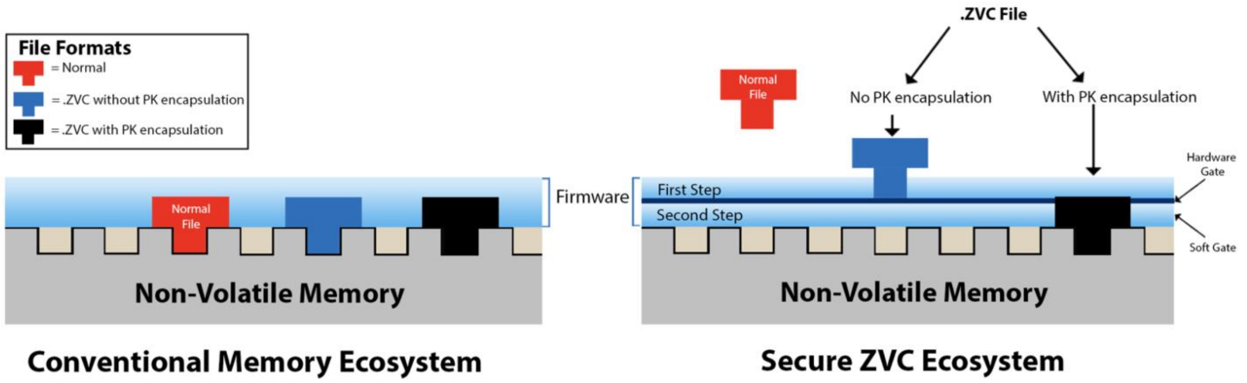


Figure 4. Hardware- and firmware-level exclusion of non-native data by ZVC to obliterate the attack surface

4.2. Solid-State Software on a Chip (3SoC) and Potential Quantum Resistance

The legacy computer architecture is traditionally layered, allowing permissions across these layers, which introduces complexities akin to the multiple moving parts of electronic devices from the pre-solid-state era [14]. In contrast, the 3SoC abstraction of the proposed ZVC ecosystem consolidates all these layers by prohibiting third-party permissions. This approach eliminates vulnerabilities associated with permissions, effectively reducing the attack surface to zero, similar to the solidity and simplicity of solid-state electronics [22].

The 3SoC abstraction of the ZVC ecosystem not only enhances portability but also improves robustness, energy efficiency, and resilience.

Currently, a consortium focused on 3SoC is validating its hypothesis in minimalist IoT device settings and extending its design attributes to mainstream computers for implementing ZVC. This involves integrating a switchable 3SoC module into a NAND non-volatile flash memory chip, which can be seamlessly integrated into any legacy computer motherboard via standard data ports, as illustrated in Figure 5.

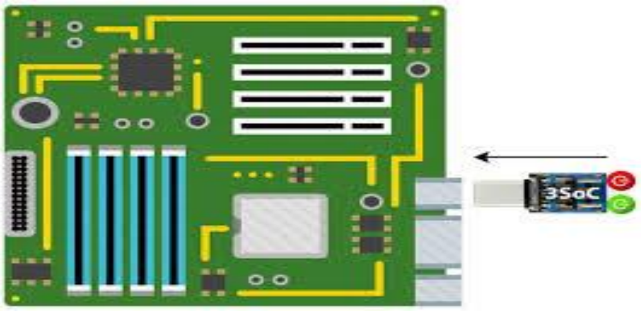


Figure 5. Integration of switchable 3SoC module with a computer motherboard

The legacy computer motherboard depicted in Figure 5 can be found in various forms such as laptops, desktops, or remote servers. This versatility enables the engineering of both 3SoC client computers and 3SoC servers, facilitating the creation of a 3SoC network. This network functions as a completely secure, malware-proof, and quantum-resistant intranet, effectively isolating all adversary client devices (Figure 6).

The 3SoC network achieves robust security by completely prohibiting third-party permissions. Moreover, its design is encryption-agnostic at the human-computer interface level, which enhances its conceptual resistance against quantum threats. Further details on this are elaborated in the following section.

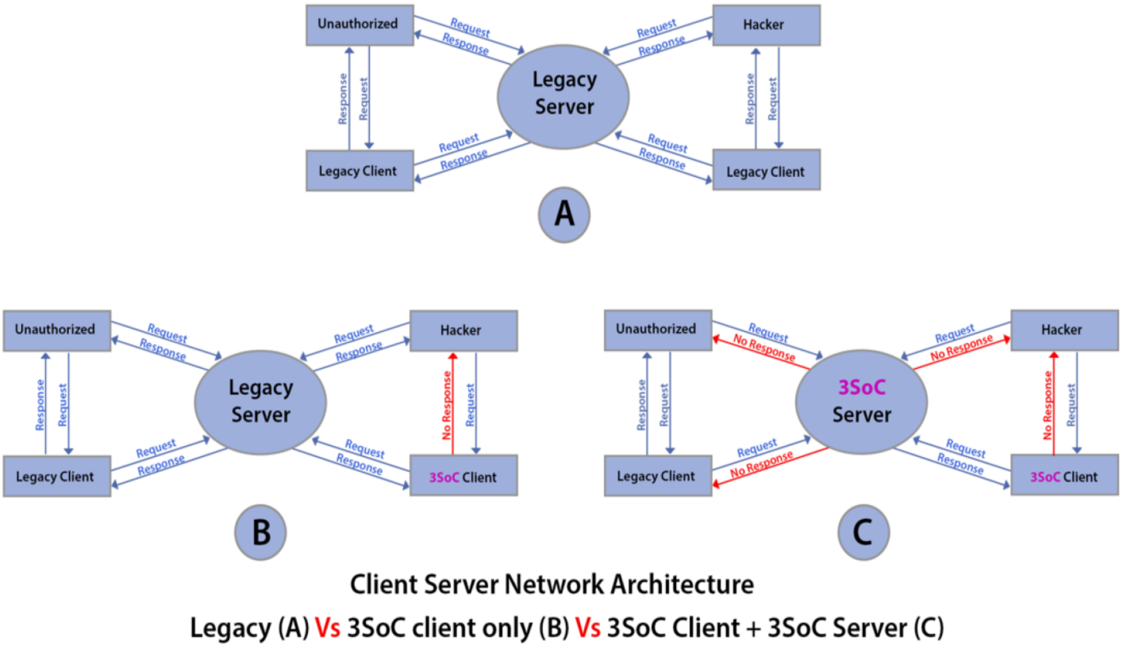


Figure 6. Three scenarios of client–server network architecture: (A) legacy, (B) 3SoC client only, and (C) 3SoC client + 3SoC server (intranet)

V. SUPREMACY AND THE Q-DAY THREAT

Quantum technology is advancing rapidly as companies compete to achieve quantum supremacy, promising a drastic reduction in computing time from years to mere hours or minutes. This advancement holds tremendous potential for industries reliant on data-intensive tasks, such as pharmaceuticals, artificial intelligence, industrial design, logistics, and national security [31]. However, it also poses serious cybersecurity threats to classical computing devices.

The advent of quantum computers threatens classical cryptography algorithms, rendering them vulnerable to quantum attacks. The anticipated "Q-Day" marks the hypothetical moment when quantum computers could potentially disrupt the Internet [4], which could have catastrophic implications given the widespread use of cryptographic schemes in everyday online activities.

Google's announcement of quantum supremacy in 2019, demonstrating the ability to solve a problem in three minutes that would take a classical computer over a thousand years, underscores the reality of quantum computing's capabilities [33]. However, achieving the millions of qubits necessary to break modern cryptography remains a formidable challenge. Practical quantum computers with such capacity could compromise nearly all modern public-key cryptographic systems.

To mitigate these risks, preparations are underway for quantum-safe cryptographic algorithms, tools, techniques, and deployment strategies to safeguard classical ICT infrastructure before quantum computers reach operational capacity.

5.1. Potential Quantum Computing Business Model

It is estimated that breaking classical encryption will require around 317 million qubits [34], each currently costing approximately USD 10,000 [35]. Even with expected cost reductions, the expense of an encryption-breaking quantum computer would remain exorbitant, likely requiring a business model akin to cloud-based computing dominated by Amazon/AWS (33%) [36].

This scenario implies that quantum computing will likely be accessible only through Quantum Computing Service Providers (QCSPs), not as personal desktop versions due to cost prohibitions. This limitation, while advantageous in preventing widespread access, also simplifies regulation efforts for standard-setting bodies like NIST in the US and ENISA in Europe. These agencies focus on developing standards for regulating QCSPs, ensuring they adhere to guidelines that mitigate risks associated with quantum computing services.

While current efforts focus heavily on PQC (post-quantum cryptography) standards, despite many candidate algorithms failing initial reviews by NIST [20, 21], regulatory agencies continue drafting technical standards for QCSP operations. These standards aim to withstand the decryption capabilities of powerful quantum computers and safeguard classical computers from future quantum threats.

In light of these developments, it is crucial to explore alternatives beyond PQC to ensure comprehensive protection against potential quantum hacking scenarios.

5.2. Securing Quantum Computing Service Provider (QCSP) Network

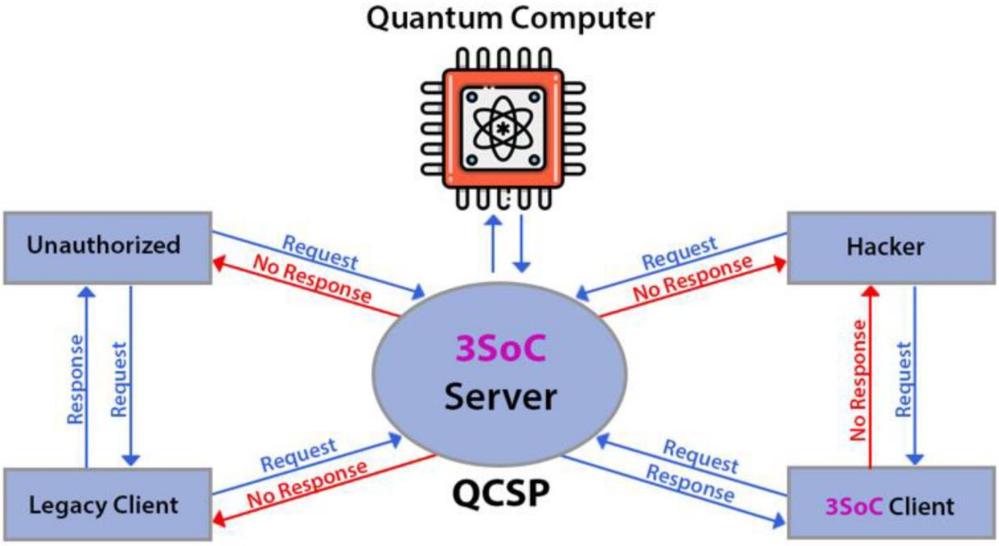


Figure 7. Quantum computer service provider (QCSP) providing quantum computing via 3SoC Intranet to subscribers

Figure 7 illustrates the typical operations of a Quantum Computing Service Provider (QCSP), which offers cloud-based quantum computing services akin to contemporary cloud computing providers. Subscribers to these services are equipped with a 3SoC client as part of their service agreement.

Access to the quantum computing resources provided by the QCSP is routed through a 3SoC server. This server exclusively processes authentication requests originating from authenticated 3SoC client devices. Requests from non-subscribers or legacy computing devices are systematically rejected. Therefore, the implementation of a 3SoC intranet presents a robust defense against potential misuse of quantum computing technology by malicious entities, even in scenarios where Post-Quantum Cryptography (PQC) algorithms may not fully mitigate risks.

VI. LIMITATIONS AND CAVEATS

This paper introduces and provides theoretical support for two new hypotheses currently under investigation. These hypotheses could significantly impact our understanding of solid-state electronics, computer hardware/software, and particularly enhance security and resilience in building a robust Internet. However, caution is warranted when extrapolating the conclusions of this report to real-world scenarios due to the following reasons:

- The hypotheses are based on empirical data primarily from a limited-use hardware wallet experiment [14] and require validation across diverse mainstream computing environments before broader application.
- Ongoing research on ZVC/3SoC means that conclusions drawn from available data are preliminary and subject to updates as more information becomes available.
- Currently, cloud services appear to be the most feasible route for making quantum computing accessible to end-users in the foreseeable future.
- 3SoC devices inherently restrict the porting of generic or non-compliant third-party peripheral devices [27].
- Further rigorous experimentation by peer researchers is necessary to test, validate, or refute the hypotheses related to ZVC/3SoC and replicate the findings.
- It is essential to establish appropriate key performance indicators (KPIs) to quantify and qualify the case studies designed to investigate these formulated hypotheses.

Despite these limitations, this study presents compelling evidence that quantum-safe security for computing devices is theoretically achievable through an encryption-agnostic approach. ZVC represents a novel method for securing future computers, potentially making them quantum-resistant. The 3SoC abstraction of ZVC also supports the possibility of de-layering legacy computer architectures to enhance and replicate the robustness, energy efficiency, portability, and resilience observed in solid-state devices.

VII. CONCLUSION

Quantum computing (QC) is an emerging and rapidly advancing field [37]. With the potential to break RSA and ECC algorithms, nearly all encrypted Internet traffic could be impacted. Businesses worldwide are investing heavily in advancing QC knowledge and practices. McKinsey forecasts significant benefits for first-wave industries from QC as early as 2025 [37]. Quantum algorithms already exist for major public-key cryptosystems, and their complete decryption seems inevitable.

The urgency to mitigate the QC threat is clear. Without the NIST PQC selection process, many candidate algorithms would have received minimal scrutiny and might have been adopted as proprietary encryption methods. The fact that several algorithms tested by NIST have been cracked, yet are still in commercial use (e.g., Rainbow in ABCmint cryptocurrency and SIKE by AWS, Cloudflare, and Google [38, 39]), underscores the critical need for alternative cybersecurity strategies.

As the quantum computing industry leans towards Quantum as a Service (QaaS) as the predominant business model, the feasibility of bad actors owning highly expensive quantum computers is remote. This suggests that malicious use of quantum computing against victims will likely occur through QaaS providers. Therefore, the best approach to mitigate impending quantum threats to the Internet is to segregate subscription-based quantum computing activities from the mainstream Internet, regulating QaaS access rather than attempting individual protection of each Internet-connected device. The 3SoC consortium is actively exploring such quantum sequestration strategies to safeguard against potential quantum computer threats.

While the ZVC-powered 3SoC network architecture is still in development as a robust cybersecurity framework, its early adoption within the cybersecurity research community will accelerate validation and standardization. This offers an alternative to the vulnerable legacy computing infrastructure that currently supports a multi-trillion-dollar cybercrime industry. It also presents new avenues to address recent PQC failures in preparing for impending quantum threats. This paper aims to stimulate interest among cybersecurity researchers and cryptographers to critically evaluate the encryption-agnostic approach of ZVC/3SoC through rigorous testing and validation of its quantum-safe hypothesis.

VIII. REFERENCES

[1] Preskill, J. Quantum computing 40 years later. arXiv 2021, arXiv:2106.10522.

[2] Arute, F.; Arya, K.; Babbush, R.; Bacon, D.; Bardin, J.C.; Barends, R.; Martinis, J.M. Quantum supremacy using a programmable superconducting processor. Nature 2019, 574, 505–510. [CrossRef] [PubMed]

[3] Bova, F.; Goldfarb, A.; Melko, R.G. Commercial applications of quantum computing. EPJ Quantum Technol. 2021, 8, 2. [CrossRef] [PubMed]

[4] Castelvecchi, D. The race to save the Internet from quantum hackers. Nature 2022, 602, 198–201. [CrossRef] [PubMed]

[5] Steve, M. Cybercrime to Cost the World $10.5 Trillion Annually by 2025. Cybercrime Magazine. 13 November 2020. Available online: https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021 (accessed on 8 August 2022).

[6] Cornea, A.A.; Obretin, A.M. Security Concerns Regarding Software Development Migrations in Quantum Computing Context; Department of Informatics and Economic Cybernetics, Bucharest University of Economic Studies: Bucharest, Romania, 2002; Volume 5, pp. 12–17, ISSN 2619-9955. [CrossRef]

[7] Rozell, D.J. Cash is king. Nature 2022, 16, 2022. [CrossRef] [PubMed]

[8] De Wolf, R. The potential impact of quantum computers on society. Ethics Inf. Technol. 2017, 19, 271. [CrossRef]

[9] Grimes, R.A. Cryptography Apocalypse: Preparing for the Day When Quantum Computing Breaks Today's Crypto; John Wiley & Sons: Hoboken, NJ, USA, 2019.

[10] Schiffer, B.F. Quantum computers as an amplifier for existential risk. arXiv 2022, arXiv:2205.02761. 11. Casati, N.M. Use of Quantum Computers in Understanding Cultures and Global Business Successes. In Culture in Global Businesses; Palgrave Macmillan: Cham, Switzerland, 2021; pp. 77–103.

[11] Scott, F., III. A Buyer's Guide to Quantum as a Service: Qubits for Hire. Available online: https://www.zdnet.com/article/abuyers-guide-to-quantum-as-a-service-qubits-for-hire/ (accessed on 21 May 2021).

[12] Sharma, S.K.; Khaliq, M. The role of quantum computing in software forensics and digital evidence: Issues and challenges. Limit. Future Appl. Quantum Cryptogr. 2021, 169–185.

[13] Raheman, F.; Bhagat, T.; Vermeulen, B.; Van Daele, P. Will Zero Vulnerability Computing (ZVC) Ever Be Possible? Testing the Hypothesis. Future Internet 2022, 14, 238. [CrossRef]

[14] Alagic, G.; Alagic, G.; Alperin-Sheriff, J.; Apon, D.; Cooper, D.; Dang, Q.; Smith-Tone, D. Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process; US Department of Commerce, National Institute of Standards and Technology: Washington, DC, USA, 2019. Available online: https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=927303 (accessed on 8 August 2022).

[15] Hoschek, M. Quantum security and 6G critical infrastructure. Serb. J. Eng. Manag. 2021, 6, 1–8. [CrossRef]

[16] Lennart, B.; Benjamin, K.; Niko, M.; Anika, P.; Henning, S. When—And How—To Prepare for Post-Quantum Cryptography. McKinsey Digital. 4 May 2022. Available online: https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/when-and-how-to-prepare-for-post-quantum-cryptography (accessed on 8 August 2022).

[17] Computer Security Research Center. Post Quantum Cryptography PQC: Workshops and Timeline. NIST; 7 July 2022. Available online: https://csrc.nist.gov/Projects/post-quantum-cryptography/workshops-and-timeline (accessed on 8 August 2022).

[18] Edlyn, T. The NIST Announcement on Quantum-Resistant Cryptography Standards is Out. Act Now! Cryptomathic. 6 July 2022. Available online: https://www.cryptomathic.com/news-events/blog/the-nist-announcement-on-quantumresistant-cryptography-standards-is-out.-act-now (accessed on 8 August 2022).

[19] Mathew, S. Encryption Meant to Protect Against Quantum Hackers is Easily Cracked. New Scientist. 8 March 2022. Available online: https://www.newscientist.com/article/2310369-encryption-meant-to-protect-against-quantum-hackers-is-easily-cracked/ (accessed on 28 May 2022).