World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(REVIEW ARTICLE)

Check for updates

What comes after Moore's Law: A comprehensive review of emerging computing paradigms

Benita Urhobo [1, *] and Dumebi Ugwuegbulam [2]

[1] *Department of Computer Science, Western Illinois University, Macomb, Illinois, United States.*
[2] *Department of Information Technology, University of the Cumberlands, Williamsburg, Kentucky, United States.*

World Journal of Advanced Research and Reviews, 2024, 24(03), 2997-3007

Publication history: Received on 23 November 2024; revised on 29 December 2024; accepted on 31 December 2024

Article DOI: https://doi.org/10.30574/wjarr.2024.24.3.4033

Abstract

As Moore's Law continues to dictate exponential increases in computing power over the past few decades, hardware architectures are beginning to encounter physical limits that threaten the pace of progress. Microchip components have decreased in size to atomic scales, requiring advanced manufacturing techniques that drive up costs and introduce new obstacles. While Moore's Law has remarkably held true since its proposal in 1965, recent years have seen a diminishing rate of advancement as further size reductions become exponentially more challenging. As a result, researchers are exploring innovative computational approaches and technologies to continue advancing performance beyond traditional silicon-based transistors. This comprehensive review explores the physical barriers threatening Moore's Law's sustainability and investigates potential post-silicon alternatives in domains like quantum computing, neuromorphic architectures, and optical switching. The review finds that emerging technologies show promise in addressing specific computational problems but are not yet capable of fully replacing conventional digital systems. A hybrid model combining traditional and novel models may be needed to ensure ongoing gains in performance, albeit at a slower pace than silicon's historic trajectory.

Keywords: Quantum; Neuromorphic; Photonic; Three-dimensional; Moore's Law; Integrated Circuits; Transistors; computing; Capabilities; Emerging; Technologies; Paradigms; Commercial Adoption; applications; Machine Learning; Simulation; Silicon

1. Introduction

As transistor dimensions shrink to atomic scales and quantum effects increasingly disrupt conventional semiconductor behavior, Moore's Law's exponential pace of progress is grinding to a halt. Gordon Moore originally predicted that the number of transistors on integrated circuits would double every year but later revised this to every two years (Mack, 2011). Remarkably, this observation held predominantly true for over five decades as components shrank in size according to periodic table parameters (Keyes, 2006). However, silicon's miniaturization is nearing fundamental limits as the sizes of transistors approach the uncertainty threshold where quantum properties invalidate classic semiconductor physics models (Schaller, 1997). At such small scales, electrons can no longer be fully confined, tunneling between components undermines logic functions, and thermal challenges intensify (Lundstrom, 2003). While lithographic and manufacturing advances enabled ongoing reductions until recently, costs and difficulties have accelerated dramatically, necessitating alternative approaches to continuing advancing performance capabilities beyond traditional Moore's Law scaling. This comprehensive review aims to analyze the physical barriers threatening Moore's Law's sustainability and investigate emerging computational technologies that may prolong growth in processing power and datacenter capabilities. By exploring options in quantum, neuromorphic, and photonic

* Corresponding author: Benita Urhobo

computing, this review will assess their potential for addressing Moore's exponential trajectory's halting and determine if they are capable of fully replacing conventional silicon architectures.

2. Emerging Technologies for Supplementary Computing

Computing technologies are rapidly evolving to supplement conventional von Neumann architectures addressing their intrinsic limitations. Novel paradigms inspired from nature showcase promising approaches harnessing alternative physics. Near-term prototypes indicate such unconventional substrates may excel for certain problems over general-purpose computers. Photonic networks [1], quantum machines [2], and brain-inspired hardware possess distinguishing attributes from digital computers. This section explores three emerging computing models and their potential roles.

2.1. Photonics for Data Transportation

2.1.1. Advantages of Photonics

Photonics has several advantages over traditional electronic communication. Photons can carry significantly more data than electrons as they do not interact with each other, allowing for higher bandwidths [1]. Optical signals experience less attenuation and are less susceptible to interference, making photonic networks more robust over long distances. Moreover, data transmission via light is nearly instantaneous while electrons incur delays, thereby reducing latency for time-sensitive applications.

Silicon photonics promises to alleviate electronic interconnect bottlenecks. Complex integrated photonic processors combining optical and electronic components on a chip could facilitate multi-terahertz on-chip communication [2]. They would eliminate the need for separate electronic and optical devices, reducing size and power consumption. Furthermore, integrating high-speed photonic links into VLSI chips could boost inter-chip bandwidths between processors and memory by several orders of magnitude.

Optical communication requires new photonic device technologies to generate, guide and detect light on ultrasmall footprints compatible with CMOS processing [2]. Significant progress has been made in developing efficient light sources like LEDs and lasers, low-loss waveguides and high-performance photodetectors. Advances in nanophotonic structures and materials are pushing the boundaries to tightly confine and route photons on integrated circuits.

2.1.2. Research in Silicon Photonics

Researchers worldwide are working towards fully monolithic silicon photonic processors [3]. They aim to co-optimize photonic, electronic and thermoelectric components to maximize the hybrid system's capacity. Significant progress has been made in demonstrating basic building blocks like ring resonators, modulators and detectors on CMOS-compatible silicon substrates.

Advances in silicon photonics have also enabled sophisticated photonic circuits mimicking electronic signal processing functions. For instance, optical add-drop multiplexers, switches and filters have been realized that can implement routing primitives [4]. Polarization handling through silicon nanostructures also allows complex polarization manipulation.

Silicon foundries have started mass producing integrated photonic platforms [4]. This allows leveraging the scalability of CMOS processing to yield compact, inexpensive photonic devices. Commercialization efforts aim to manufacture higher component densities and integrate transistors with optical waveguides for photonic-electronic cooperation.

Overcoming loss in silicon continues to be addressed through novel low-loss waveguide designs and heterogenous integration with higher index-contrast materials. Thermo-optic tuning of resonators has also enabled reconfigurable and feedback-based systems on chip. Such advances synergize photonics with electronics to utilize their relative strengths optimally.

2.1.3. Applications of Optical Neural Networks

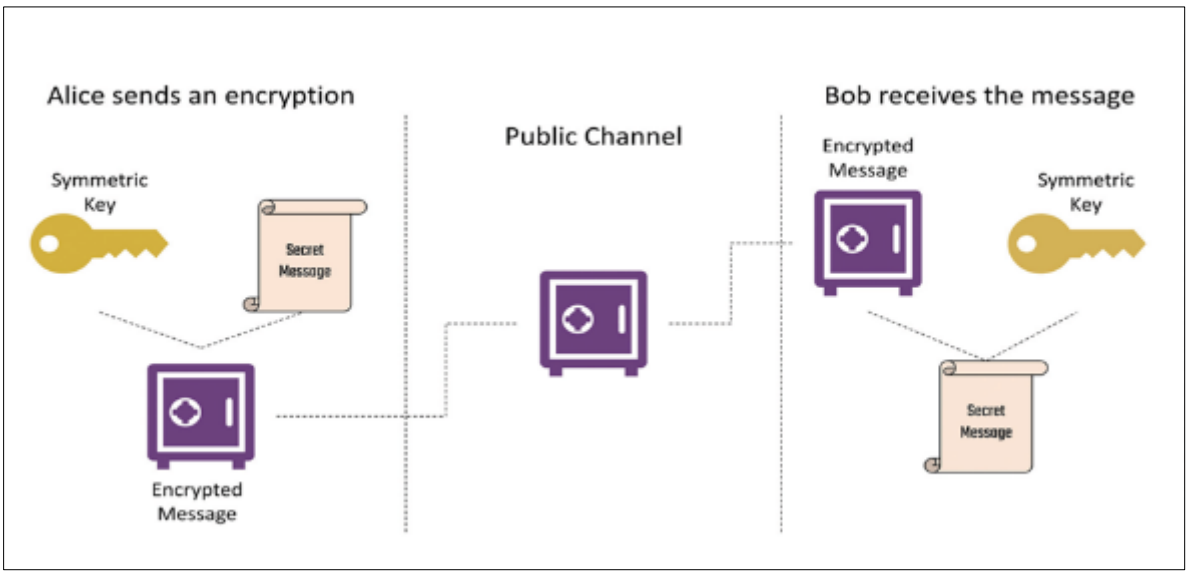
Neuromorphic photonics provides an appealing approach to overcome electronic von Neumann bottlenecks for neural networks. Photonic neurons can emulate biological spiking dynamics with analog circuits operating at teraops speeds [5]. Integrating such circuits with learning algorithms offers highly efficient inference and training. Optical circuits can represent weights and activations of neural networks using light pulses. Recent demonstrations have implemented perceptrons and multilayer feedforward networks to recognize patterns. Photonic neurons with nonlinearity and

configurable weights allow complex receptive field modelling. Interconnecting numerous photonic neurons with programmable quantum-dot cellular automata circuits provides a route to scalable photonic spiking networks [5]. Their asynchronous, event-based operation mimics the brain more closely than conventional von Neumann architecture. Overcoming noise and device non-idealities remains an active area of research. Photonic implementations also need hybridization with electronics for programming and memory. Nonetheless, they present a compelling approach for cognitive workloads beyond the capabilities of directly transposing neural networks to silicon.

2.2. Quantum Computing for Specialized Simulations

2.2.1. Quantum Advantage for Simulation

Quantum computers possess attributes allowing efficient simulation of quantum systems through harnessing quantum mechanical principles such as superposition and entanglement.[6] Algorithmic approaches for example Harrow-Hassidim-Lloyd are designed to simulate dynamics without enumerating multifarious potential state combinations which would be cumbrous for classical computers, furnishing a likely speedup.[7] Such intrinsic edge aids addressing certain problems quantum processors are best structured for that classical devices face difficulties with.



Source; https://www.cryptoquantique.com/blog/post-quantum-cryptography/

Figure 1 Post Quantum

Quantum simulation proves advantageous for modeling phenomena governed by quantum mechanics as variables magnify, incorporating materials structure-property relations contingent on minute subsystem interactions [7]. Analyzing molecular docking, which aids pharmaceutical development, requires incorporating quantum-level details at the atomic scale. This makes certain problems impossible to solve using classical computation alone.

Initial intermediate-scale quantum devices have run simulations rendering experiments unachievable by traditional computing, evidencing quantum simulation capacities ahead of full fault-tolerance [8]. While imperfect, these substantiate progress towards generative large-scale quantum simulation. Continued scaling and algorithmic resilience to noise are important to harness nearer-term practical advantage.

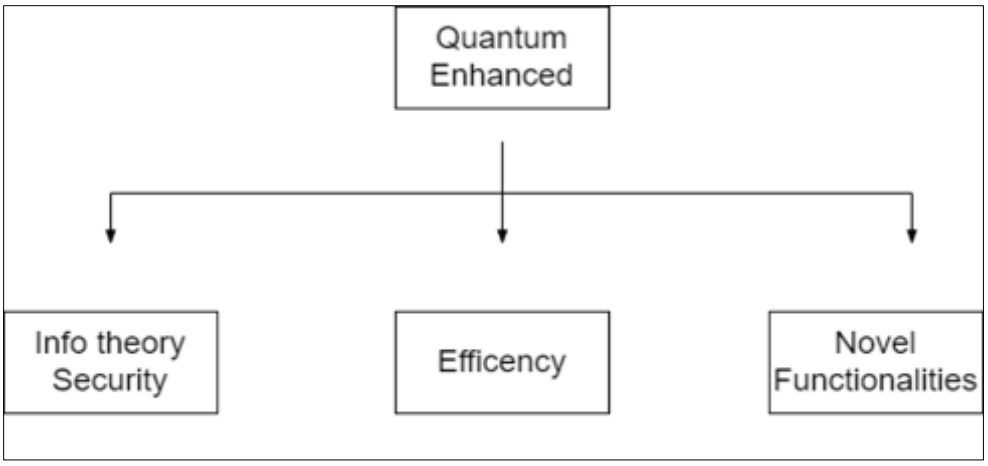


Figure 2 Quantum Enhanced

2.2.2. Role in Materials and Drug Discovery

Quantum simulators support computational materials and drug design research accelerating discovery through reduced costs and lead times [8]. Modeling candidate systems facilitates preempting performances and behaviors before expensive physical experimentation, complementing prevailing frameworks with an apt technology for elaborate electronic structure simulations.

High-throughput screening of huge chemical spaces requires hierarchical virtual screening campaigns aided by predictive insights such as properties across diverse candidate databases, supplemented by computational hypothesis generation complementing characterization approaches [9]. Pharmaceutical R&D equally involves modeling drug-target interplay quantum mechanically at the molecular scale. Quantum simulations can facilitate property profiling beneficial for optimization, assisted by calibrated binding energies and interaction characterization [10].

2.3. Neuromorphic Computing for Pattern Recognition

2.3.1. Hardware Implementation of Neural Networks

Dedicated neuromorphic hardware implements neural networks using specialized analog circuits that functionally mimic the neurons and synapses of the biological brain [10]. Key examples are IBM's TrueNorth and Intel's Loihi chips containing millions of low-power artificial neurons connected massively in parallel through on-chip learning and memory structures, similarly to natural neural tissue [11].

Their non-von Neumann architecture co-locates memory and computation to facilitate convolutional and recurrent network functionality using energy-efficient asynchronous circuits [12]. Elements such as crossbar arrays with tunable resistive elements represent weights through locally modification of conductances. Such brain-inspired systems improve the efficiency and throughput of inference and learning tasks compared to general von Neumann platforms by avoiding bottlenecks arising from separating memory and processing. Their specialized design processes inputs and learns in a massively parallel manner akin to biological neural systems.

2.3.2. Advantages over Conventional Computing

Neuromorphic computing architectures provide intrinsic benefits over digital von Neumann systems for artificial intelligence workloads through specialized in-memory learning processes and massively parallel analog circuits emulating the human brain [12]. Bio-synchronous adaptive hardware mimics natural synaptic strengthening and weakening to efficiently learn decision functions directly from high-dimensional raw data in power-efficient accelerated manners not possible with software simulations [12].

Low-power "in-memory" learning through locally modifying conductances between co-located weighted neuron connections lowers energy and latency overheads from costly data movement between separate processing and memory units as in conventional architectures [13]. Asynchronous event-driven "spiking" dynamics additionally capture temporal aspects important for sequential prediction that deep neural networks struggle to learn.

Dedicated neuromorphic substrates support unconventional learning rules better optimized for temporal or sparse data like Spike-Timing Dependent Plasticity with locally-modifiable synapses [13]. This allows for applications beyond image recognition, using time-encoded or event-driven sensors to provide real-time intelligence, even under strict energy and connectivity constraints.

2.3.3. Applications in Edge Intelligence

Compact power-efficient neuromorphic processors are uniquely placed to meet the stringent size, latency and throughput needs of embedding intelligence directly at edge devices [14]. Embedded adaptive classifiers and controllers minimize transmission of raw data to remote cloud platforms.

Applications such as predictive maintenance of industrial machinery, smart home appliances, and personalized health monitors benefit from real-time distributed intelligence implemented locally using brain-inspired learning chips [14]. Edge deployment also enhances response times for time-critical tasks like autonomous vehicles or emergency response systems [14]. Localized learning preserves privacy by keeping sensitive data and decisions on-device, avoiding cloud dependencies which consume remote server resources and introduce latencies unacceptable for low-level automation requiring millisecond reactions. Neuromorphic edge computing unlocks new applications through optimized hardware adapted to constrained smart edge nodes.

3. Challenges to Commercial Adoption

This section aims to analyze the key challenges facing the commercial adoption of emerging computing paradigms discussed earlier. Despite their promise, novel technologies must overcome hurdles to viability at scale for real-world use. The following subsections explore issues in photonic, quantum, and neuromorphic computing that research is addressing to make them competitive alternatives.

3.1. Remaining Roadblocks in Silicon Photonics

3.1.1. High Cost of Manufacturing

While progress has been made in developing photonic components compatible with CMOS infrastructure, their manufacturing processes require additional lithography steps and materials increasing costs compared to traditional electronics [15]. Complex multilayer fabrication of complex integrated silicon nanophotonic circuits with heterogeneous integration of lasers, modulators and detectors inevitably results in higher chip real-estate usage [15]. This challenges photonic solutions from achieving price points acceptable for widespread commercialization unless production yields and throughput can match established electronic manufacturing techniques.

Researchers are exploring several approaches to reduce manufacturing costs for silicon photonics. One approach involves developing photonic platforms that leverage shared electronic fabs and infrastructure to benefit from existing mass manufacturing capabilities and economies of scale [16]. Foundries are also optimizing photonic fabrication processes and introducing design rules to streamline integration of multiple photonic elements. Advances in low-cost materials like polymers and hybrid integration of active elements are being explored as well.

3.1.2. Maintaining Coherence

Scaling quantum devices requires maintaining quantum coherence across a growing number of fragile and error-prone qubits [17]. However, interactions with the environment inducing decoherence prove challenging to mitigate as more qubits are integrated on a chip. Thermal fluctuations, electromagnetic interference and manufacturing defects diminish coherence initially attainable in smaller prototype systems. Substantial engineering remains to sufficiently isolate growing qubit networks from decohering influences.

Techniques like error correction codes and dynamic decoupling pulses are being explored to counter environmental noise [17]. Architectural approaches involve compartmentalizing regions conducting quantum operations from noisy interfaces. Nanophotonic interconnects integrating photon sources on chip for long-distance entanglement enable distributed quantum computing approaches as well [17]. Advanced materials like isotopically purified silicon help minimize nuclear spin interactions.

3.1.3. Manufacturing Variability

Uniformity across large quantities of quantum components is harder to achieve than classical chips given quantum phenomena's sensitivity [18]. Small manufacturing variations in qubit or readout parameters can induce errors not

tolerable given requirements for strong coherence. This leads to lower yields worsening with increasing scale. Improved fabrication precision and design margin are required to produce quantum chips matching the quality levels accessible now only in smaller test systems.

Promising avenues involve developing modular, plug-and-play quantum hardware for scaling, informed by classical approaches like socketing chips [18]. Neuroinspired approaches extract useful computations from inconsistent quantum arrays as well. Quantum dots and donor spins in silicon benefit from atomic-level precision while superconducting circuits require micron-scale homogeneity. Development of manufacturing techniques for various physical implementations remains important.

3.2. Barriers in Commercial Neuromorphic Systems

3.2.1. Algorithmic Development

Mainstream machine learning techniques like backpropagation are difficult to directly apply on neuromorphic substrates requiring alternative algorithms adapted to their unconventional in-memory learning dynamics [19]. Developing training methods optimized for brain-inspired systems, sparse or temporal data remains active research preventing widespread usage. Retraining existing deep networks on neuromorphic chips also poses issues from non-digital nature.

Research into neuromorphic-optimized algorithms is making progress in developing unsupervised methods, and local learning rules inspired by neuroscience. Spike-based temporal learning approaches like spike-timing dependent plasticity and localization rules show promise. Hybrid approaches also utilize neuromorphic hardware as an accelerator for convolution operations within deep learning workflows.

3.2.2. Device Variability

Maintaining consistency across resistive devices emulating synapses remains problematic given nonlinear conductive elements exhibit intrinsic variability affecting network functionality [19]. Lifespans too vary demanding sophisticated ways calibrating or replacing degraded cells without losing memory. Increased scale exacerbates inconsistencies requiring solutions like adaptation or ensemble computation.

Device and material research aims to improve uniformity, endurance and tolerating defects through novel memristive technologies [19]. On-chip adaptive algorithms accommodate variability through lifetime calibrating degraded cells. Architecture approaches map synaptic functions across networks of devices increasing tolerance. The system-level design incorporates intrinsic device variations [26].

Experimental demonstrations on neuromorphic testbeds help validate algorithms on non-ideal hardware prior to commercialization. Testing across realistic device variation scenarios supplements characterization on ideal simulations. Such co-validation helps establish reliability and consistency expectations for neuromorphic systems [20].

3.2.3. Software Environment

Software frameworks for neuromorphic systems lag compared to GPUs due to their non-von Neumann nature [20]. Programming tools facilitating algorithm development, network specification, calibration and management across diverse neuromorphic architectures are nascent. Application deployment also faces issues since neuromorphic results may not precisely replicate traditional systems necessitating co-design of software and hardware [20]. Overall software issues limit adoption despite progress in chips.

New programming models are emerging for brain-inspired hardware, adopting declarative approaches inspired by neuroscientific descriptions over traditional imperative programming. Development of domain-specific languages and compiler workflows help automate mapping tasks to hardware. Integrated development environments enable neuromorphic application prototyping through visual programming and simulation.

4. Quantum Computing and its Role in Addressing Cybersecurity Challenge

Quantum computing presents promising opportunities to address limitations in computational power but also introduces significant cybersecurity risks that will need to be managed. While still in early stages of development, quantum computers have the potential to disrupt existing cryptographic systems and challenge traditional notions of cybersecurity if deployed for malicious purposes [24]. The purpose of this section is to explore the potential

cybersecurity implications of quantum computing and outline some of the challenges and mitigation approaches as the technology continues to progress. It examines the impact on cryptography, risks to quantum systems and infrastructure, challenges of attributing quantum attacks, and the ongoing research needed to secure both classical and quantum technologies as quantum computing capabilities increase.

4.1. Implications for Cryptography

4.1.1. Threat to Asymmetric Encryption

Existing public-key cryptography schemes like RSA that underpin much of our online security infrastructure are vulnerable to attacks from quantum computers. Shor's algorithm allows factors of large numbers to be determined exponentially faster on a quantum computer compared to classical techniques [21]. This poses a major threat to the security assumption that factoring large integers is computationally infeasible. The nature of Shor's algorithm exposes the underlying mathematical structure of RSA, showing that polynomial time quantum factoring renders the encryption insecure [27]. An additional concern is that a sufficiently powerful quantum computer could be used to efficiently calculate discrete logarithms, breaking schemes based on the difficulty of that problem like Elliptic Curve Cryptography.

Researchers are exploring alternatives to RSA that could be quantum-secure. One approach is to use algorithms based on lattice-based cryptography, where the security comes from solving hard problems on lattices or multidimensional grids of points. Another option is hash-based digital signatures that rely on the one-way property of cryptographic hash functions. Both of these approaches could provide security against quantum attacks like Shor's algorithm and may form the basis for post-quantum signature schemes and encryption standards.

4.1.2. Impacts on Symmetric Cryptography

Grover's algorithm also compromises the security of cryptographic hash functions and symmetric ciphers by allowing an unknown value to be found in quadratic time rather than exponential time, reducing the key size needed to provide equivalent security [21]. Popular techniques like the Advanced Encryption Standard (AES) could become crackable with a large enough quantum computer. Grover's algorithm enables an exponential speedup over classical brute force attacks by allowing a value to be found with approximately square root of the number of trials. While symmetric schemes may still provide security against weaker quantum adversaries, longer keys will be needed to safeguard against more powerful quantum computers, [26].

Symmetric algorithms like AES will remain a relevant part of post-quantum security architectures, but key sizes may need to be doubled to compensate for Grover's algorithm. For example, transitioning from 128-bit keys to 256-bit keys could help maintain an equivalent level of protection against both classical and quantum threats, [27]. The performance and communication overhead of using increased key sizes will require careful consideration.

4.1.3. Transitioning to Post-Quantum Cryptography

In response, cybersecurity efforts are focused on developing new post-quantum cryptographic algorithms that are secure against both classical and quantum attacks [21-23]. Standards setting bodies like NIST are running competitions to identify new public-key encryption, digital signature and key establishment schemes suitable for deployment once quantum computers become a threat. While post-quantum cryptography provides a potential solution, transitioning existing systems will require significant effort. It will be a major undertaking for industry and governments to update algorithms, replace keys and modify protocols on internet-scale systems to ensure continuity of cryptographic services in a post-quantum world [27].

Implementing post-quantum solutions will likely occur in phases over many years. An initial focus may be on high value systems like certificate authorities and root key infrastructure. Over time, updated algorithms could be integrated into mainstream applications, services and protocols on a prioritized schedule. Standards organizations will need to provide guidance on transition best practices, interoperability testing, and coordination between developers and vendors.

4.2. Managing other Quantum Computing Security Risks

4.2.1. Securing Quantum Devices and Infrastructure

As quantum computing hardware expands, security risks will emerge from physical access to quantum devices, connectivity between quantum and classical systems, and human operators with access to fragile quantum states [22-23]. Countermeasures are needed to protect quantum processors, interconnects, and cryogenic facilities from tampering and safeguard quantum information during storage and transmission. Quantum processors require

extraordinary control and isolation from environmental interference to function properly. Protecting these delicate systems and the quantum information they contain from potential attackers will necessitate new physical and procedural security controls.

Some possible controls include restricted access zones around quantum equipment, tamper-evident enclosures, sensor monitoring for anomalies, and air-gapped security architectures separating quantum and internet-connected systems. Personnel security will also play a key role in mitigating insider threats and protecting sensitive Quantum computing developments. Physical protection challenges may be one of the hardest issues facing the integration of quantum abilities into real-world technology.

4.2.2. Detection of Quantum Attacks

Quantum adversaries may attempt to subvert computations or extract sensitive data using techniques like embedding hidden messages in quantum states or using measurement results to gain information [23]. Techniques for validating the proper functioning of quantum systems and detecting such interference must be developed. As the field progresses, new quantum-based forms of malware, sabotage and espionage may emerge that are difficult to recognize using classical tools alone. Quantum-secure monitoring and auditing methods will help guarantee the sanctity of quantum computations and confidentiality of quantum data.

Quantum watermarking and fingerprinting techniques show promise for detecting unauthorized interference or counterfeit quantum states. For example, subtle changes could be made to a target quantum state that reveal its origin or intended recipient when later detected. Ongoing research is refining such approaches to catch tampering, characterize the capabilities of quantum adversaries and establish legal and technical frameworks for a new era of quantum network security monitoring.

4.2.3. Attribution and Response Challenges

Determining the origin of quantum attacks poses unique challenges due to the difficulty of monitoring quantum communications and establishing reliable forensic evidence at the quantum level [23]. Countries will need to work together to attribute attacks, coordinate vulnerability disclosures, and formulate proportionate responses against the use of quantum resources for malicious cyber activities. International cooperation on legal authorities and response playbooks will become increasingly relevant as the security implications of quantum technologies continue to emerge.

Effective response will require tracing quantum capabilities back to their real-world sources through technological and intelligence means. International law and policy approaches must also be established to enable legal jurisdictions over quantum systems and activities that cross borders. As with other emerging technologies, cooperation between governments, researchers and industry will be key to enacting responsible and proportionate measures against those misusing quantum abilities

5. Enabling Secure Applications of Quantum Technologies

While quantum computing introduces new security challenges, it also enables innovative solutions if properly safeguarded. Realizing quantum technology's benefits will require addressing both offensive and defensive security concerns.

5.1. Opportunities in quantum cryptography

5.1.1. Quantum Key Distribution

Quantum key distribution (QKD) allows the generation of secure encryption keys with information-theoretic security through the transmission of encrypted quantum states [23]. By detecting any potential eavesdropping or distortion of the quantum channel, QKD ensures the detected keys are secure against even a quantum computer. Early QKD networks have been deployed and seen increasing commercial adoption offering benefits over classical key distribution techniques [24]. As QKD network infrastructure expands to more users, techniques for integrating quantum keys with existing security protocols must mature to ensure compatibility and trust [25].

QKD uses properties of quantum mechanics like quantum entanglement and measurement to detect any interference, however channel noise and instability also impact security. Ongoing engineering research aims to extend maximum transmission distances, improve sensitivity to intrusion attempts and develop robust key management to maintain

security over long time periods [24]. Standardized testing frameworks help characterize real-world performance of QKD systems to identify weaknesses and facilitate adoption.

5.1.2. Quantum signatures

A promising post-quantum signature scheme is based on the security of quantum one-way functions using superposition and measurement [23]. By signing quantum states of information rather than classical bits, signature forgery could be detected on verification through quantum effects. Quantum signature approaches may one day augment or replace traditional public key infrastructures and provide a more robust foundation for attributing digital communications [25].

One challenge is developing practical signature schemes requiring feasible operations on large quantum systems while guaranteeing unforgeability. Recent theoretical prototypes leveraging quantum annealing or trapped ions have shown promise but require far greater qubit counts and controls before scaling to real-world applications [23]. Considerable research persists to refine the underlying quantum algorithms, error-correction approaches, and physical implementations of quantum-based signature techniques.

5.2. Defensive applications in quantum cryptography

5.2.1. Quantum watermarking

By encoding messages within subtle quantum properties, watermarking techniques can detect tampering of quantum communications and computation [24]. For example, an author's quantum watermark embedded in a state allows verification of origin and alteration. When applied to valuable quantum computations like optimizer results, watermarking provides a way to establish proof of provenance [25]. However, more research is still needed to refine host encoding, extraction, and tamper detection given noise in realistic quantum systems.

Additionally, technical and legal frameworks must account for the implications of quantum watermarks interacting with principles like fair use and establishment of liability. International norms will play an important coordinating role to balance protection, open access, and responsible research as the power of quantum systems grows. Watermarking demonstrates quantum mechanics' potential to enable new forms of copyright and authentication compared to classical systems alone.

5.2.2. Quantum data encryption

Quantum cryptography techniques like quantum one-time pads provide information-theoretically secure schemes to encrypt data transmitted through quantum channels [23]. While practical challenges persist in generating, transmitting and storing large volumes of quantum encrypted data, theoretical approaches show promise [24]. Machine learning algorithms have also been explored that natively operate on encrypted quantum data without decryption, enabling privacy-preserving applications [25].

However, integrating quantum encryption into classical systems requires hybrid techniques. Homomorphic encryption utilizing both quantum and classical resources offers a path to fully homomorphic encryption of both types of data [23]. Improving the efficiency and scale of quantum data encryption aligns with defensive needs around privacy and sensitive information protection in the rapidly advancing field of quantum information science

6. Conclusion

Conclusively, while Moore's Law has remarkably shaped the development of the semiconductor industry for decades, continuous progress at its historic pace is rapidly nearing its physical limits. Increasingly smaller manufacturing processes require enormous costs and resources. Innovations such as chiplet integration, 3D chip stacking, new computing models like quantum and brain-inspired technologies offer promising strategies to enhance computing power beyond conventional scaling. However, widespread adoption of these emerging technologies still faces substantial challenges. Their full capabilities to replace digital electronics are still unclear. Therefore, hybrid systems integrating classical and novel computational paradigms may be necessary to maximize benefits. Sustained efforts in research and development across computing sectors will be vital to secure continued technological advancement in the post-Moore's Law era.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Keyes, R. (2006). The Impact of Moore's Law. IEER Solid-States Society Newsletter. 11(3). 25- 27. https://doi.org/0.1109/N-SSC.2006.4785857

[2] Lundstrom, M. (2003). Moore's Law Forever? Science, 299(5604), 210–211. https://doi.org/ 10.1126/science.1079567

[3] Mack, C. A. (2011). Fifty Years of Moore's law. IEEE Transactions on Semiconductor Manufacturing, 24(2), 202–207. https://doi.org/10.1109/tsm.2010.2096437

[4] Meng, L., Xin, N., Hu, C., Sabea, H. A., Zhang, M., Jiang, H., Ji, Y., Jia, C., Yan, Z., Zhang, Q., Gu, L., He, X., Selvanathan, P., Norel, L., Rigaut, S., Guo, H., Meng, S., & Guo, X. (2022). Dual-gated single-molecule field-effect transistors beyond Moore's Law. Nature Communications, 13(1). https://doi.org/10.1038/s41467-022-28999-x

[5] Schaller, R. R. (1997). Moore's law: Past, present and future. IEEE Spectrum, 34(6), 52–59. https://doi.org/10.1109/6.591665

[6] Sridhar, Arvind et al. "3D-ICE: Fast Compact Transient Thermal Modeling for 3D ICs with Inter-tier Liquid Cooling." Proceedings of the 2010 International Conference on Computer- Aided Design, 2010, EPFL. https://infoscience.epfl.ch/record/149790?ln=en. Accessed 4 March 2023.

[7] Hunter, M., et al. "Special Session: Test Challenges in a Chiplet Marketplace." 2020 IEEE 38th VLSI Test Symposium, 4 June 2020, IEEE Explore. Accessed 4 March 2023.

[8] Preskill, J. (2018). Quantum Computing in the NISQ era and beyond. Quantum, 2, 79.

[9] Computer and Telecommunications. (2011, November 28). Research and development of photonic computer[J]. Retrieved March 5, 2023, from https://d.wanfangdata.com.cn/periodical/gddnydx201111027

[10] Shalf, J. M., & Leland, R. (2015). Computing beyond moore's law. Computer, 48(12), 14–23. https://doi.org/10.1109/mc.2015.374

[11] Sui, C. (2022). Semiconductor physics. Electronic Devices, Circuits, and Applications, 35–39. https://doi.org/10.1007/978-3-030-80538-8_3

[12] Rashid, S., Shakeel, R., & Bashir, H. (2016). Moore's Law Effect on Transistors Evolution. International Journal of Computer Applications Technology and Research, 5(7), 495–499. https://doi.org/10.7753/IJCATR0507.1014

[13] Waldrop, M. M. (2016). The chips are down for Moore's law. Nature, 530(7589), 144–147. https://doi.org/10.1038/530144a

[14] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Communications of the ACM, vol. 21, no. 2, pp. 120–126, 1978.

[15] P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," in Proceedings 35th annual symposium on foundations of computer science, 1994, pp. 124–134.

[16] A. A. Abushgra, "Variations of QKD Protocols Based on Conventional System Measurements: A Literature Review," Cryptography, vol. 6, no. 1, p. 12, 2022, [Online]. Available: https://doi.org/10.3390/cryptography6010012

[17] Ladd, T. D., Jelezko, F., Laflamme, R., Nakamura, Y., Monroe, C., & O'Brien, J. L. (2010). Quantum computers. Nature, 464(7285), 45-53.

[18] J. Houle and D. Sullivan, "Eight Bit Quantum Fourier Transform Using the FDTD Method," 2021 IEEE Workshop on Microelectronics and Electron Devices (WMED), Boise, ID, USA

[19] Nielsen, M. A., & Chuang, I. L. (2010). Quantum computation and quantum information. Cambridge university press.

[20] F. Bova, A. Goldfarb, and R. G. Melko, "Commercial applications of quantum computing," EPJ Quantum Technol., vol. 8, no. 1, p. 2, Dec. 2021, doi: 10.1140/epjqt/s40507-021-00091-1.

[21] W. Buchanan and A. Woodward, “Will quantum computers be the end of public key encryption?,” Journal of Cyber Security Technology, vol. 1, no. 1, pp. 1–22, Jan. 2017, doi: 10.1080/23742917.2016.1226650.

[22] P. Wallden and E. Kashefi, “Cyber security in the quantum era,” Commun. ACM, vol. 62, no. 4, pp. 120–120, Mar. 2019, doi: 10.1145/3241037.

[23] F. Bova, A. Goldfarb, and R. G. Melko, “Commercial applications of quantum computing,” EPJ Quantum Technol., vol. 8, no. 1, p. 2, Dec. 2021, doi: 10.1140/epjqt/s40507-021-00091-1.

[24] W. Buchanan and A. Woodward, “Will quantum computers be the end of public key encryption?,” Journal of Cyber Security Technology, vol. 1, no. 1, pp. 1–22, Jan. 2017, doi: 10.1080/23742917.2016.1226650.

[25] P. Wallden and E. Kashefi, “Cyber security in the quantum era,” Commun. ACM, vol. 62, no. 4, pp. 120–120, Mar. 2019, doi: 10.1145/3241037

[26] Innocent O. Asevameh, Oladipupo M. Dopamu, & Joseph S. Adesiyan. (2024). Enhancing resilience and security in the U.S. power grid against cyber-physical attacks. World Journal of Advanced Research and Reviews, 22(2), 1043-1052. https://doi.org/10.30574/wjarr.2024.22.2.1535

[27] Oladipupo M. Dopamu, "Cloud - Based Ransomware Attack on US Financial Institutions: An In - depth Analysis of Tactics and Counter Measures", International Journal of Science and Research (IJSR), Volume 13 Issue 2, February 2024, pp. 1872-1881, https://www.ijsr.net/getabstract.php?paperid=SR24226020353