RP Current Trends In Engineering And Technology (e-ISSN: 2583-5491)
Vol. 4, No. 3 (July – September 2025) pp. 46–49

RESEARCH PLATEAU PUBLISHERS

Cite this article: S. Chollangi, Advanced quantum materials for secure quantum computing and cyber security, *RP Cur. Tr. Eng. Tech*. **4** (2025) 46–49.

Original Research Article

Advanced quantum materials for secure quantum computing and cyber security

Sriharsha Chollangi*

Department of Electrical Engineering, Gannon University, USA
*Corresponding author, E-mail: chsriharsha15@gmail.com

ARTICLE HISTORY
Received: 4 April 2025
Revised: 27 June 2025
Accepted: 27 June 2025
Published: 3 July 2025

KEYWORDS
Quantum materials;
Secure computing;
Superconducting qubits;
Quantum cryptography;
Quantum key distribution;
Post-quantum security.

ABSTRACT
The swift evolution of quantum computing demands the development of advanced quantum materials to enhance qubit stability, coherence time, and fault tolerance. Materials such as superconducting Josephson junctions, silicon-based quantum dots, and rare-earth ion-doped crystals play a crucial role in optimizing quantum processors. These materials are being engineered to minimize decoherence and maximize quantum error correction, enabling scalable and efficient quantum computing systems. Simultaneously, the rise of quantum technologies presents both challenges and opportunities in cyber security. Traditional encryption methods, such as RSA and ECC, are susceptible to quantum attacks, forcing the advancement of post-quantum cryptographic solutions. Quantum key distribution (QKD) and lattice-based encryption leverage quantum mechanics to create asecure channel for communication, ensuring resilience against quantum threats. This paper examines the latest breakthroughs in quantum materials and their implications for secure quantum computing and cyber security. By bridging materials science with cryptographic advancements, this study aims to establish a robust foundation for quantum-secure communication networks and computing platforms.

1. Introduction

1.1 Quantum computing

Quantum computing is a type of computing that merges with the principle of quantum mechanics with computational theory to solve problems beyond the access of classical computers. In1980s, physicist Richard Fenman proposed the idea of following the quantum system using the quantum computer, which recognized the boundaries of classical systems in the modeling quantum phenomenon [1]. This concept was developed by David Deutush, who presented the concept of a universal quantum computer [2]. In the 1990s, quantum field gained momentum due to the development of the Quantum algorithm of Peter Shor, which can create a sharp factor compared to the most famous classical algorithm, which highlights the ability to calculate quantum in cryptography [3]. Quantum computers work using quantum bits, or qubits, that takes the advantage of superposition and entanglement to perform complex calculations parallelly. Below Table 1 shows a high -level difference between quantum and classical computing [4].

Table 1: High -level difference between quantum and classical computing [4].

Quantum Computing	Classical Computing
qubits – these can be 0,1 or both at the same time.	bits -these can be either 1 or 0.
Computational power increases exponentially with count of qubits	Computational power increases at 1:1 ratio with count of transistors
Rate of errors is high	Rate of errors is low
Used for complex simulation, data analysis and optimization problems	Used for day-to-dayprocessing.

Despite the error correction and significant challenges in qbit stability, the advancement in quantum materials continues to carry forward the boundaries of quantum computing.

1.2 Key factors for performance

The key factors that can contribute to the performance of the quantum chips.

Qubit Stability: This is defined on how efficiently a qubit can maintain the quantum state over time without getting corrupted by external influences. If qubits aren't stable the quantum computation becomes unreliable. The stability of qubits is important for the running longer algorithms and reducing the errors [5].

Coherence time: This is defined how long a qubit quantum state **(**like superposition or entanglement) is maintained before losing the information due to environmental interactions that the qubit is in. The quantum operation must be completed within the coherence time, else the decoherence ruins the computation. The longer the coherence time the more reliable the quantum circuit can be [5].

Fault tolerance: This is defined as the ability of a quantum computer to continue tooperate correctly, even when some of its qubits experiences any errors [5].

The specialized quantum materials form the foundation for the qubit design the directly influencing the stability, coherence and error rates. To build a scalable and fault -tolerant quantum chips, ongoing research must focus on discovering and refining the materials that can sustain the coherent quantum behavior.

2. Quantum materials

When we think of future of quantum computers, there are three important technologies that are helping to make it real. First, we have Superconducting Josephson Junctions. These are tiny circuits that work only at super cold temperatures, close to absolute zero. They help create the basic building blocks of qubits, by using special electrical properties that only show up when materials have zero resistance. Next, silicon-based quantum dots. These are like little "traps" that hold single electrons, using their spin to store information. These are made with the similar technology that is used to make current computer processors, which makes it easier to scale up and could fit into existing tech more smoothly. And third, we have rare-earth ion-doped crystals. These crystals can hold quantum information for a long time without fading away. That makes them perfect for things like quantum memory, which is essential for future quantum networks. The three technologies used by some of the big companies is shown in Figure 1 [6] and Table 2 shows the materials that are commonly used for each technology. Each of these approaches brings something different and together, they're paving the way to the quantum future.

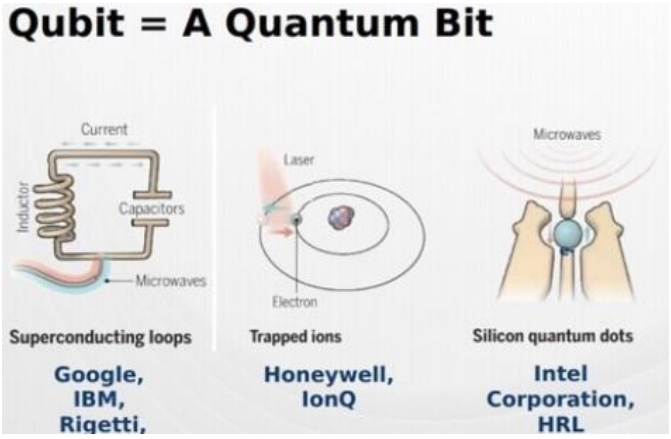

Figure 1: Three technologies used by some of the big companies.

Table 2: The materials that are commonly used for technology.

Technology	Example Materials	Role in Quantum Computing
Superconductors	Aluminum (Al), Niobium (Nb)	Josephson junctions in superconducting qubits [7][8]
Semiconductors	Silicon (Si), Silicon-Germanium (SiGe)	Spin qubits in quantum dots [9]
Rare-Earth Doped Crystals	Europium-doped Yttrium Orthosilicate (Eu^{3+}:Y_2SiO_5)	Ultra-long-lived quantum memory, quantum repeaters [10]

Quantum computing has a great capacity of solving very complicated problems. But to unlock its potential, we must overcome serious technical challenges. The two major obstacles that stand in the way are environmental noises and material imperfections. Qubits are extremely sensitive to their surroundings. Even slight interference from temperature changes, electromagnetic filed changes, radiations can disrupt the state of the qubit. Coming to the materials, tiny flaws in the materials that are used to build the qubits can lead to instability and errors, making the computation unreliable. To overcome these two major issues, researchers are working on the Advance fabrication techniques, refining how pure the qubits are being built and implementing quantum error corrections. Using the purer materials and cleaner process can reduce the imperfections and improve the performance of the qubits. To implement the quantum error correction additional qubits needs to be used. So they can detect and fix the errors without compromising the quantum state, allowing computations to continue accurately despite noise. These solutions are leading to more stable and scalable quantum systems. As fabrication improves and error correction becomes more efficient, quantum computers will be moving closer to real-world applications. The following Table 3 shows the quantum chips developed by some of the major companies [11-20], and the qubit count of the respective quantum chip.

Table 3: The quantum chips developed by some of the major companies [11-20].

Company	Chip Name	Qubit Count
IBM	Eagle	127
IBM	Osprey	433
IBM	Condor	1121
Google	Sycamore	53
Google	Bristlecone	72
Microsoft	Majorana 1	8
Intel	Tunnel Falls	12
Rigetti	Aspen-M	80
Rigetti	Aspen-11	40
D-Wave	Advantage	5760
IonQ	Aria	25
IonQ	Harmony	11
Quantinuum	H1-1	32
Quantinuum	H1-2	32
Quantinuum	H2-1	32
Alibaba	Tai Zhang	11
Baidu	Qianshi	10

3. Quantum computing and cyber security challenges

Once the quantum computers are fully established, they will be able to break most commonly used encryption methods like RSA and ECC algorithms that currently protect everything from personal emails to national security systems. These current encryption methods mainly rely on mathematical approach that are nearly impossible for current computers to crack. But, quantum machines can crack them in a fraction of the time with Shor's algorithm. In the Table 4 you can see the different RSA Key size, their respective security level and the common usage.

The cyber attackers can save the sensitive encrypted data now, they could decrypt it in the future once quantum computing becomes powerful enough. This is why the rise of quantum computing is not just going to be a huge technological rise, but a global cyber security crisis, unless we shift to quantum immune cryptographic systems and post quantum cryptographic solutions, that can withstand any kind of attacks from the quantum computers. Below are couple of such solutions that are being actively worked on.

Table 4: The different RSA key size, their respective security level and the common usage.

RSA Key Size	Security Level	Usage
1024-bit	❌ *Insecure*	Deprecated — can be broken with enough classical resources
2048-bit	✅ *Standard Secure*	Most commonly used today (e.g., HTTPS, SSL certificates)
3072-bit	🔒 *High Security*	For higher-security applications
4096-bit	🛡️ *Very High Security*	Rare, due to performance cost

Quantum Key Distribution (QKD) works on the principles of quantum mechanics to generate and securely deliver the cryptographic keys even with if someone tries to eavesdrop [21], as shown in Figure 2. In this approach, if there is any attempt to hack the key, the key transmission quantum state gets disturbed and that will alert the receiver and the sender, and. This makes it theoretically unbreakable and ideal for high-security communications.

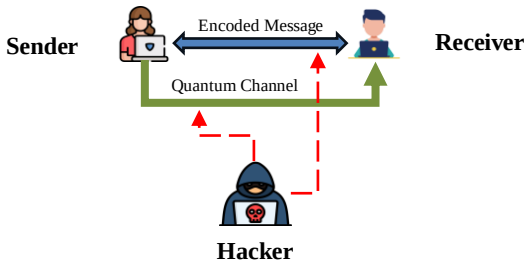

Figure 2: Principles of quantum mechanics to generate and securely deliver the cryptographic keys.

Lattice-Based Encryption a type of cryptographic system where the security relies on the presumed hardness of lattice problems such as the Shortest Vector Problem (SVP) and the Learning With Errors (LWE) problem [22]. This is one of the strongest post quantum techniques. It is built on complex mathematical structures that even quantum computers find difficult to solve efficiently. Lattice based schemes are not only just secured from quantum computing but also very adaptable. Standards bodies like NIST (National Institute of Standards and Technology) are working in the direction of identifying and selecting quantum safe algorithms. Apart from QKD and Lattice Based encryption, there are other evolving methods such as hash-based signatures and code-based encryption [23-25]. These are being actively studied to ensure our cyber security systems remain robust in the long term, even against future quantum threats.

4. Conclusions

In quantum materials, we're seeing breakthroughs that are pushing the limits of coherence, control, and scalability that are opening the doors for stable and powerful quantum systems. On the cyber security front, post quantum cryptographic algorithms are being regulated to defend against risks that can be caused by quantum computers, guaranteeing the long-term data security. Looking ahead, the focus is shifting toward scalable quantum computing, building systems that go beyond the lab and into real-world application. Along with that, next-generation encryption techniques must be robust enough to secure critical infrastructure in a post-quantum world. One key takeaway is that no single discipline can solve these complex challenges alone. The challenges we face demand interdisciplinary collaboration. Continuing the collaboration and innovation, will unlock new breakthroughs in quantum materials and post quantum cryptographic solutions to build a secure, scalable quantum future.

Authors' contributions

The author read and approved the final manuscript.

Conflicts of interest

The author declares no conflict of interest.

Funding

This research received no external funding.

Data availability

No new data were created.

References

[1] R.P. Feynman, Simulating physics with computers, *Int. J. Theor. Phys.* **21** (1982) 467–488.
[2] D. Deutsch, Quantum theory, the Church–Turing principle and the universal quantum computer, *Proc. Royal Soc. London, A. Mathemat. Phys. Sci.* **400** (1985) 97–117.
[3] P.W. Shor, Algorithms for quantum computation: Discrete logarithms and factoring, *Proc. 35th Annual Symposium on Foundations of Computer Science, IEEE* (1994) 124–134.
[4] P. Upama, F. Hossain, Md Jobair, M. Nazim, M. Masum, et al., Evolution of Quantum Computing: A Systematic Survey on the Use of Quantum Computing Tools (2022).
[5] E.G. Rieffel, H.P. Wolfgang, *Quantum Computing: A Gentle Introduction*, MA: MIT Press, Cambridge (2011).
[6] https://www.hpcwire.com/2020/08/19/intel-connects-the-quantum-dots-in-accelerating-quantum-computing-effort/
[7] M. Kjaergaard, M.E. Schwartz, J. Braumüller, P. Krantz, J.I.-J. Wang, S. Gustavsson, W.D. Oliver, Superconducting qubits: Current state of play, *Annu. Rev. Cond. Mat. Phys.* **11** (2020) 369–395.
[8] IBM Quantum. (n.d.), *IBM Quantum Experience*. https://quantum-computing.ibm.com/
[9] F.A. Zwanenburg, A.S. Dzurak, A. Morello, M.Y. Simmons, L.C.L. Hollenberg, D.N. Jamieson, S. Rogge, Silicon quantum electronics, *Rev. Mod. Phys.* **85** (2013) 961–1019.
[10] A. Kinos, *Light-Matter Interaction and Quantum Computing in Rare-Earth-Ion-Doped Crystals*, Lund University (2018).
[11] IBM, IBM Quantum Roadmap, IBM Research (2023). https://research.ibm.com/blog/quantum-roadmap.
[12] F. Arute, K. Arya, R. Babbush, et al., Quantum supremacy using a programmable superconducting processor, *Nature* **574** (2019) 505–510.
[13] Microsoft, Azure Quantum and Topological Qubits.' Microsoft Research (2023). https://www.microsoft.com/en-us/quantum
[14] Intel, Intel Unveils Tunnel Falls Quantum Chip, Intel Newsroom (2023). https://www.intel.com/content/www/us/en/newsroom/news/intel-unveils-tunnel-falls-quantum-chip.html.
[15] Rigetti, Aspen-M Quantum Processor, Rigetti Computing

(2023). https://www.rigetti.com.
[16] D-Wave Systems, Advantage Quantum Computer, D-Wave (2023). https://www.dwavesys.com
[17] IonQ, IonQ Aria: High-Fidelity Quantum Computing, IonQ (2023). https://ionq.com/technology.
[18] Quantinuum, H-Series Trapped-Ion Quantum Computers, Quantinuum (2023). https://www.quantinuum.com/hardware
[19] Alibaba DAMO, Alibaba Quantum Lab Develops Tai Zhang, Alibaba Group (2022). https://damo.alibaba.com
[20] Baidu, Baidu Releases Qianshi Quantum Chip, Baidu News (2022). https://www.baidu.com/news
[21] NIST IR 8105: Report on Post-Quantum Cryptography. https://doi.org/10.6028/NIST.IR.8105
[22] D. Micciancio, O. Regev, Lattice-based Cryptography: In: *Post-Quantum Cryptography*, Springer (2009) pp. 147–191.
[23] D.J. Bernstein, J. Buchmann, E. Dahmen, (Eds.), *Post-Quantum Cryptography*, Springer (2009).
[24] L. Chen, et al., *Report on Post-Quantum Cryptography*, NISTIR 8105 (2016). https://doi.org/10.6028/NIST.IR.8105
[25] NIST Post-Quantum Cryptography Project. https://csrc.nist.gov/projects/post-quantum-cryptography