RP Current Trends In Engineering And Technology (e-ISSN: 2583-5491)
Vol. 4, No. 3 (July – September 2025) pp. 50–52

RESEARCH PLATEAU PUBLISHERS

Cite this article: U. Mutyala, Quantum computing materials for quantum and cyber security engineering, *RP Cur. Tr. Eng. Tech.* **4** (2025) 50–52.

Original Research Article

Quantum computing materials for quantum and cyber security engineering

Ujval Mutyala*

Department of Computer Technology, Eastern Illinois University, USA
*Corresponding author, E-mail: ujvalroy@gmail.com

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

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

ABSTRACT
Quantum computing positioned to transform computational resources by providing exponential power for problem solving. However, quantum technologies research introduces opportunities and risks in the cyber security field. The advancement in quantum computing materials plays a crucial role in stablilizing quibits, decoherence and error correction keys. Materials such as superconductors, semiconductors, topological insulators and nitrogen-vacancy centers (NV) in diamonds have shown significant potential to improve quantum computing processes. In the scope of cyber security field, materials and quantum resistant encryption methods are essential for mitigating threats from quantum attacks on classical cryptographic protocols. The emergence of post quantum cryptography (PQC) and quantum distribution of keys (QKD) depends on robust quantum materials to ensure secure communication. This research explores the latest advancements on quantum materials, along with its impact on quantum computing hardware and its implications. By integrating quantum materials with quantum methodologies will address the computational power of quantum technologies and the risk they introduce.

1. Introduction

Encryption is the key cornerstone of secure communication, which ensures the confidentiality, integrity and authenticity of data [1].The encryption rely on mathematical problems deemed computationally infeasible for classical computers, such as factoring large prime numbers or elliptic curver discrete algorithms. However the quantum computers works on the principles like superposition and entanglement which threatens the classical computing algorithms making these methods absolute. This article will explain the role of quantum computing materials and their advancements with a paradigm shift in the computational power.

2. Fundamentals of encryption and quantum threats

In classical computing there are two types of encryption mechanisms.

2.1 Symmetric key encryption

Symmetric key encryption uses single shared key for encrypt and decrypt (Figure 1).In this mechanism the key that used to encrypt the data is shared with the other entity in order to decrypt the data. The overall security depends on key length and complexity [2]. Encryption keys with bit sizes: Advance Encryption Standard (AES) with bit sizes AES-256, AES-128.

2.2 Asymmetric key encryption

Asymmetric encryption employs two keys i.e. public and private key pairs (Figure 2). The public key is used to encrypt the data before it was sent to other entity and once the end user receives the data will decrypt it using private key [2]. This type of encryption provides high security when compared with symmetric encryption. The security relies on the mathematical intractability. Some of encryption keys with bit sizes: Rivest-Shamir-Adleman RSA -256 & RSA -128, Elliptic Curve Cryptography ECC.

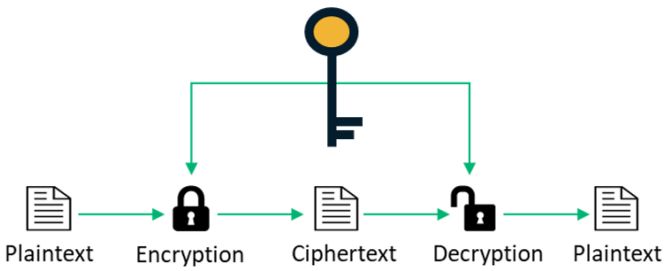

Figure 1: Symmetric key encryption.

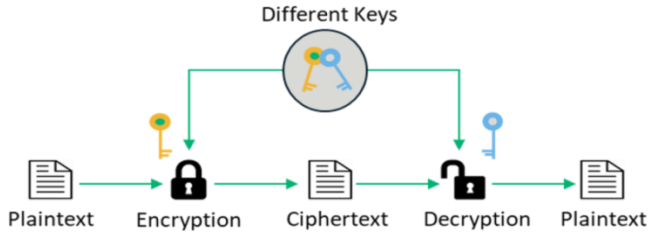

Figure 2: Asymmetric encryption employs two keys i.e. public and private key pairs.

2.3 Quantum threats to encryption

Quantum algorithms like Shor's algorithm can factorize large prime integers in a exponentially faster than the classical methods which leads breaking RSA and ECC asymmetric key encryptions [3]. Whereas, the Grover's algorithms can accelerates brute-force attacks on symmetric key halving the

key sizes i.e. AES-256 becomes equivalent to AES-128 [4]. These quantum algorithms could decrypt the sentive data, breach network communications, and undermined the puble-key infrastructure (PKI).

The quantum computers leverage qubits that helps enhancing computational power for certain problems. The qubits are very unstable that requires specialized materials for stabilizing and mitigating decoherence.

3. Quantum computing materials: Enabling stable qubit operations

The performance of quantum systems relys on the materials that preserve qubits coherence and enabling error correction. The key advancements include:

3.1 Superconducting materials

The materials used in the quantum computers are directly impact the efficiency, scalability and real-word deployments. The cryptographic landscape shits due to the the potential threats of quantum attacks making material science as a key factors in the future of security. The superconduction qubits are key for very large scale quantum computers. These qubits rely on materials that exhibit superconductivity at very low temperature, reducing energy loss and increase in stability [5]. The choice of materials affects the coherence time, error rates and the overall compurational efficiency. IBM and Google both conducted extensive research into the use of key materials like Niobium (Nb), Aluminium (Al), and Titanium Nitride (TiN) in quantum computing.

Table 1: The key properties of Niobium (Nb), Aluminum (Al), and Titanium Nitride (TiN) in the context of quantum computing materials:

Property	Niobium (Nb)	Aluminum (Al)	Titanium Nitride (TiN)
Temperature (Tc)	~9.2 K	~1.2 K	~5 K – 6 K
Coherence in Qubits	Used in transmon and flux qubits due to high Tc and low losses	Common in superconducting qubits (e.g., transmons) due to ease of fabrication	Low-loss material suitable for resonators and qubit shielding
Junction Usage	Used in superconducting quantum circuits	Primary material for Josephson junctions	Emerging alternative for durable superconducting layers
Mechanical Properties	High hardness and good ductility	Soft, easy to pattern	Hard and wear-resistant
Application in Quantum Computing	Superconducting qubits, resonators	qubit capacitors	Low-loss superconducting resonators

IBM's Research

Titanium Nitride (TiN): IBM demonstrate dusing TiN in qubits that significantly enhances coherence times [6]. The qubits are constructed using TiN capacitors which allows relaxation and dephasing times upto 60 microsecounds. This represents major fold of improvement over those made with traditional aluminium. This improvement helped to reduce losses from the two level systems at interfaces.

Niobium (Nb): IBM also explored niobium-germanium structures for superconducting quantum devices [7]. This hybrid superconductor-semiconductor junctions show promising low losses to coherence in the qubits that leverages Nb as favourable superconducting properties.

Google's Research

Aluminium (Al): Google demonstrated experiment using gate-based quantum computer where the qubits are constructed based on Aluminium [8]. The choose of materials based on the superconducting properties and reliability in qubit fabrication. Experiment demonstrated quantum computer ability to perform complex computations beyond the capabilities of classical supercomputers.

3.2 Semiconductor materials

Semiconductor qubits promise higher scalability and integration with classical computing environment. Silicon (Si) which is one of the best semiconductor material which was used for quantum computers as they can easily integrate with existing Complementary metal oxide semiconductor (CMOS) technology [9]. This compatibility makes it easier integrating with large scal quantum processors. Silicon-Germanium (SiGe) helps to enhance performance in quantum transistors by improving electron mobility.

Intel has actively advancing research in quantum computing focusing on silicon based qubit technologies.

Intel Research

Intel published research demonstrating high uniformity and control fidelity at single electron spin qubits across 300-mm wafers. It is an outstanding acheviment that underscores the potential for mass production and scaling of silicon based quantum processors using standard semiconductor manufacturing process [10].

3.3 Topological insulators

Quantum computers research using topological materials and their qubits utilizes Majorana fermions to achieve fault-tolerant quantum computing. These are more stable when compared with superconducting and semiconducting materials which helps to reduce the need for complex quantum error correction [11]. If this approach is successful that could lead to more scalable quantum computers which brings cryptographic threats sooner than expected.

Microsoft quantum computing research focuses on topological insulators and superconducting nanowires that helps to enable Majorana based qubits.

Microsoft Research

Microsoft first introduced Majorna processor which is based on topoconductor. This chip can control the Majorana particles to create reliable qubits, potentially incubating million qubits onto a single chip processor. This kind of advancement can revolutionize the computing infrastructure by enabling accurate simulations and deeper understanding at material science [12].

If Microsoft qubits succeeds, we might see fault tolorenet quantum computers that raises risk on RSA, ECC and cryptographic alogorithms at risk. Organizations should prepare for post-quantum cryptography (PQC) to mitigate the risks before these quantum computers reach commercial viability.

3.4 Nitrogen-vacancy (NV) centers in diamond

Diamonds and defect based materials enable advance quantum computing technologies especially Quantum Key Distribution (QKD). It offers unbreakable encryption using quantum mechanics. The defects centers in materials such as Nitrogen-Vacancy centers in diamonds and Silicon Carbide (SiC) defects that allow for stable quantum states. The QKD could replace the classical encryption in the future but the infrastructure challenges still remain.

National Institute of Standards and Technology (NIST) conducting research on diamond NV centers as promising technology for nanoscale magnetic measurements due to quantum spin state control and sensitivity [13].

4. Quantum materials and cyber security solutions

Quantum materials play a pivotal in developing defences against quantum threats.

4.1 Quantum key distributuin (QKD)

The QKD leverages quantum principles that enable key exchange which is immue to quantum attacks. The implementation is totally relies on the advancement of quantum materials [14].

Detectors: Superconducting nanowires can help to acheive more than 90 percent efficiency for photon detection.

Single-Photon: The NV centers in diamonds and semiconductor quantum dots can generate stable and high purity photons.

4.2 Post quantum cyyptography (PQC)

The PQC are encompasses cryptographic algorithms which are designed to resists attacks on quantum computers by safeguarding classical systems against threats like Shor's algorithm and Groover's algorithm. PQC relies on the statistical framework such as lattice based, has dhased which are standardized by NIST [15]. Quantum materials are very crucial for the deployment of PQC at large scale.

Semiconductors: Silicon (Si) materials at quantum computers help to enable efficient computation of PQC's for complex algorithms.

Quantum resistant hardware: The usage of diamond NV centers or superconducting circuits help to produce entropy for secure key strength. Innovations in the nanoscale materials are key to achieve PQC adoption to ensure compatibility with Internet of Things (IoT) and cloud infrastructure.

5. Challenges in quantum material development and implementation

There are couple of challenges during the development of quantum materials and integrations with the quantum systems.

- Decoherence and error rates: Materials should exhibit Qubit coherence times beyond milli secounds.
- Scalability: Integration of million of qubits which demands breakthroughs in nano fabrications.
- Cost and Infrastructure: The cryogenics for superconducting qubits and diamond growth at NV centers remain costly.

6. Conclusions

Material science is the key enabler for quantum security. The advancements in superconductors, semiconductors, and topological materials will define the future of secure computing. The superconducting materials is foundational for stable qubits in quantam processors. Topological materials helps to enable fault tolerant qubit resistant to decoherence. The semiconductors materials enables communications with quantum computers using quantum key distribution (QKD). The collaboration between the the cyber security professionals and material scientists is critical for development, scalability and energy efficiency. Initiatives like NIST and industry researchers should come together to bridge the gap between material science and cyber security without leaving systems vulnerable to quantum threats.

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] A. Ayub, S. Pereira, M. Thayyil, M. Ayub, From bytes to qubits: The cyber security implications of quantum advancements, *Int. J. Sci. Res. Eng. Manag.* **8** (2024) 1-5.

[2] https://sectigostore.com/blog/5-differences-between-symmetric-vs-asymmetric-encryption

[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] L.K. Grover, A fast quantum mechanical algorithm for database search, Proc. STOC (1996) 212–219.

[5] W.D. Oliver, P.B. Welander, Materials in Superconducting Quantum Bits, *MRS Bullet.* **38** (2013) 816–825.

[6] J.B. Chang, M.R. Vissers, A.D. Córcoles, M. Sandberg, J. Gao, et al., Improved superconducting qubit coherence using titanium nitride, *Appl. Phys. Lett.* **103** (2013) 012602.

[7] https://research.ibm.com/publications/evaluating-niobium-germanium-heterostructures-for-voltage-tunable-superconducting-quantum-devices

[8] https://medium.com/swlh/how-google-probably-made-the-quantum-supremacy-chip-296d5d321bbd

[9] C. Weisbuch, B. Vinter, Quantum Semiconductor Structures: Fundamentals and Applications, Elsevier (2014).

[10] S. Neyens, O.K. Zietz, T.F. Watson, et al., Probing single electrons across 300-mm spin qubit wafers, *Nature* **629** (2024) 80–85.

[11] S.-Q. Shen, Topological Insulators, Vol. 174, Springer, Berlin (2012).

[12] https://www.theverge.com/news/614205/microsoft-quantum-computing-majorana-1-processor

[13] https://www.nist.gov/programs-projects/diamond-nv-center-magnetometry

[14] S.K. Liao, W.Q. Cai, W.Y. Liu, et al., Satellite-to-ground quantum key distribution, *Nature* **549** (2017) 43–47.

[15] NIST PQC Standardization, CRYSTALS Suite, *IEEE Transactions on Quantum Engineering* (2023).