IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p-ISSN: 2278-8727, Volume 27, Issue 4, Ser. 5 (July. – August. 2025), PP 10-17
www.iosrjournals.org

Quantum Cryptography And Interdisciplinary Domains: A Literature Review On Post-Quantum Security And Quantum Communication Technologies

Srijan Seshadri

Abstract:
This literature review examines the transformative impact of quantum computing on cryptography and data security. As quantum computing technologies advance, traditional cryptographic methods face unprecedented threats, specifically from algorithms such as Shor's algorithm, which can efficiently factor large integers. This review explores post-quantum cryptography solutions, quantum key distribution protocols, quantum homomorphic encryption, and emerging quantum materials. The analysis covers fundamental quantum computing principles, quantum sensing applications, quantum communication protocols including BB84 and satellite-based QKD, and the development of quantum-resistant cryptographic systems. The review identifies noise and decoherence as one of the primary challenges limiting the practical feasibility of quantum cryptographic implementations.

Keywords: *Post-Quantum Cryptography, Quantum Computing, Quantum Homomorphic Encryption, Quantum Key Distribution, Quantum Materials*

Date of Submission: 21-08-2025 Date of Acceptance: 31-08-2025

I. Introduction

With the advent of quantum computing as a viable future of computing, many threats are posed to classical cryptography. Quantum computing, being developed to harness the power of quantum mechanics, would be able to break traditional cryptography such as RSA, which relies on factorizing, using techniques such as Shor's algorithm, which runs in polynomial time and is far more efficient than the popular classical factoring algorithm known as the general number field sieve, working in sub-exponential time [1, 2]. This has led to the requirement of post-quantum cryptography, relying on quantum mechanics and the principles of nature as we know it today instead of the mathematical computation used in its classical counterpart[3].

The idea of this research paper is to analyze the impact that quantum computing's rapid rise is having on data security, its feasibility and threat, and exploring the fundamental principles and the real-world applications of quantum technologies. We will explore concepts of quantum key distribution, discussing protocols such as the BB84, as well as satellite-based QKD. Furthermore, we will discuss homomorphic encryption in the quantum world as well.

II. Methodology

This literature review employs a systematic approach to examine the current state of quantum computing and its implications for cryptography. The methodology encompasses the following components:

Literature Search Strategy

- Primary Sources: Peer-reviewed journal articles, lectures and technical reports from quantum computing and cryptography domains
- Secondary Sources: Books, review articles, and survey papers on quantum technologies
- Time Frame: Focus on publications from 2010-2024 to capture recent developments
- Databases: IEEE Xplore, arXiv, Nature, Science, and specialized quantum computing journals

Analysis Framework

The review is structured around five key thematic areas:

- Quantum Computing Fundamentals: Basic principles, quantum gates, and algorithms
- Quantum Sensing: Applications in precision measurement and security
- Quantum Communication: QKD protocols and satellite implementations
- Quantum Materials: Superconductors, topological insulators, and their applications
- Quantum Homomorphic Encryption: Privacy-preserving quantum computation

DOI: 10.9790/0661-2704051017

Quality Assessment

Each source is evaluated based on:

- Methodological rigor and experimental validation
- Relevance to quantum cryptography applications
- Citation impact and peer review status
- Reproducibility of results and practical implications

III. Quantum Computing Fundamentals

Quantum Gates and Operations

Quantum computing exploits the fundamental quantum mechanical properties of nature in order to do computation [4]. In recent years, the field has progressed quite rapidly and is now showing the potential to outperform our current classical supercomputers. Let us now get into details about one of the key differences between a quantum computer and a classical computer.

A conventional computer uses bits, which can take the values of '0' or '1' in order to store and process information. On the other hand, however, quantum computing uses qubits or quantum bits, which work on the principle of taking any superposition of '0' and '1' [4, 5]. This allows them to access an exponentially larger Hilbert space (complex vector space that represents the state of a physical system), since 'n' qubits can be in a superposition state of 2^n possible outcomes.

Another important characteristic of quantum computing is the ability of the qubits to be in superposition, or the ability to be in multiples states at once. As an example, if a qubit is in a superposition state $|\psi\rangle$, it can be expressed as a linear combination of its basis states $|0\rangle$ and $|1\rangle$:

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

This is what allows for the exponential quantum parallelism enabling the speed of a quantum computer over a classical computer. Quantum entanglement refers to the special connection that has been made between particles such that the state of one is directly related to the state of the other, regardless of the distance between them [4, 5]. It is also central to many quantum algorithms and protocols.

Quantum Gate Operations

We will now discuss the various quantum gates used in a quantum circuit, which work similarly to logic gates in classical circuits. These transformations are accomplished unitarily and preserve the norm of the state vector of qubits, being described by unitary operators [4].

Name	Description	Action on basis states	Unitary matrix
Pauli-X Gate	Flips the state of the qubit, also known as the quantum NOT gate.	$X \lvert 0\rangle = \lvert 1\rangle$ $X \lvert 1\rangle = \lvert 0\rangle$	$X = \begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}$
Pauli-Y Gate	Introduces a phase flip along with the bit flip.	$Y \lvert 0\rangle = i \lvert 1\rangle$ $Y \lvert 1\rangle = -i \lvert 0\rangle$	$Y = \begin{bmatrix}0 & -i\\ i & 0\end{bmatrix}$
Pauli-X Gate	Inverts the phase of the qubit.	$Z \lvert 0\rangle = \lvert 0\rangle$ $Z \lvert 1\rangle = -\lvert 1\rangle$	$Z = \begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}$
Hadamard Gate	Creates a superposition of states.	$H \lvert 0\rangle = \frac{1}{\sqrt{2}} (\lvert 0\rangle + \lvert 1\rangle)$ $H \lvert 1\rangle = \frac{1}{\sqrt{2}}(\lvert 0\rangle - \lvert 1\rangle)$	$\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}$
CNOT gate	A two-qubit gate that flips the state of the second qubit (target qubit) if the first qubit (control qubit) is in the state $\lvert 1\rangle$.	$CNOT\lvert 00\rangle = \lvert 00\rangle$ $CNOT\lvert 01\rangle = \lvert 01\rangle$ $CNOT\lvert 10\rangle = \lvert 11\rangle$ $CNOT\lvert 11\rangle = \lvert 10\rangle$	$CNOT = \begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\end{bmatrix}$
Phase gate	Shifts the phase of the state $\lvert 1\rangle$ by π/2.	$S\lvert 0\rangle = \lvert 0\rangle$ $S\lvert 1\rangle = i \lvert 1\rangle$	$S = \begin{bmatrix}1 & 0\\ 0 & i\end{bmatrix}$
T Gate	Shifts the phase of the state $\lvert 1\rangle$ by π/4.	$T \lvert 0\rangle = \lvert 0\rangle$ $T \lvert 1\rangle = e^{i\pi/4}\lvert 1\rangle$	$T = \begin{bmatrix}1 & 0\\ 0 & e^{i\pi/4}\end{bmatrix}$
Swap Gate	Exchanges the states of two qubits	$SWAP\lvert ab\rangle = \lvert ba\rangle$	$SWAP = \begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 0 & 1 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\end{bmatrix}$

Shor's Algorithm and RSA Vulnerability

Algorithms evaluated by JP Morgan Chase as well as Goldman Sachs have been shown to be able to significantly reduce the time required to do complex options pricing and risk-assessment calculations. Perhaps one of the most famous and relevant examples to display the power of quantum computing is Shor's Algorithm for factorization [1, 2]. As compared to the General Number Field Sieve, a classical algorithm used for the same purpose, it is able to put up exponentially better numbers. For a comparison of their time complexities, while GNFS works in sub-exponential time, Shor's algorithm is put into the Bounded-error Quantum Polynomial Time class [1].

This has resulted in the RSA encryption algorithm becoming unsafe, and started a search for quantum-computing safe encryption [1, 2].

The RSA algorithm works as follows:

- First, choose any two large prime numbers p and q
- Next, compute n = p×q and find the totient φ(n) = (p-1)(q-1)
- Now you can choose a public exponent e
- Now, compute a private exponent d such that d×e ≡ 1 (mod φ(n))
- You can encrypt the message now: C = M^e mod n
- And decrypt using M = C^d mod n

Clearly, the RSA algorithm works on the fact that it is extremely hard to factor n. However, using Shor's algorithm, one is able to factor it out faster than classical algorithms. First, a superposition of all possible states is initialized, followed by the Quantum Fourier Transform in order to find the period of a function related to the factors of N:

$$QFT|k\rangle = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} e^{2\pi i \frac{kj}{N}} |j\rangle$$

Where N is the dimension of the Hilbert space.

Many programming frameworks already exist, some of which, such as CIRQ and Qiskit, primarily use Python to provide tools for creating and manipulating quantum circuits and running quantum algorithms. Qiskit by IBM is able to use IBM's cloud-based quantum computing.

IV. Quantum Sensing Applications

Quantum sensing exploits quantum phenomena such as entanglement, superposition, and coherence in order to measure physical quantities with extreme precision [6]. It uses quantum systems (such as spins or photons) which have been prepared into a delicate superposed state, giving them sensitivity beyond the classical limits.

The applications of quantum sensing are vast. For instance, let us consider atomic clocks: the quantum way to measure time [7]. It focuses on the atomic resonance frequencies to measure time, using atoms and lasers. It exploits the fact that atoms change energy levels when they interact with specific laser frequencies, and that response stabilizes the laser frequencies, which are then measured as the "tick" of a clock. Scientists have been able to reach incredible accuracy using this, such as the F1 Cesium clock, which has an error rate of only one second in a million years.

MRI technology also implements this, using a nitrogen-vacancy center in a diamond (made by introducing the nitrogen, which substitutes for a carbon in the diamond lattice) which can detect tiny magnetic fields from single spins [8]. Researchers have enabled high-resolution MRI on the scale of individual molecules.

These applications also exist in quantum cryptography as well. Quantum sensing techniques are being applied to better our network security. Quantum signals comprising weak photon pulses, used in QKD protocols, using quantum sensing is able to detect infrastructural tampering or eavesdropping [6]. The quantum bit error rates would be impacted, notifying users. We will be covering QKD in the next section of this paper in further detail.

V. Quantum Communication And Key Distribution

Principles of Quantum Communication

Quantum communication is the process of transmitting information using quantum states—typically photons—to guarantee the security of data. While classical communication may rely on electrical signals or light pulses without quantum properties, quantum communication uses principles of superposition and entanglement for the encoding, transmission, and decoding of the information. The sensitivity to measurement, as previously discussed, allows for great levels of security and prevents problems such as eavesdropping [9].

Entanglement helps detect eavesdropping as any disruption will disturb the entanglement, leaving a very visible trace. The seemingly "instantaneous" effect made Einstein refer to it as "Spooky Action at a Distance."

BB84 Protocol

Quantum Key Distribution (QKD) has become a significant part of the cryptographic revolution, enabling and enhancing cryptography to not rely on computational assumptions (such as the RSA relying on the fact that it is hard to factor numbers for computers), providing unconditional security [9, 10]. QKD is used to distribute encryption keys for symmetric or asymmetric ciphers, not to transmit any plain data between communication parties.

The first protocol invented was Bennett and Brassard-1984 (BB84). It is based on photon polarization. It requires the generation and detection of pulses of light in different polarizations. The encoding is stemmed from encoding the classical information in non-orthogonal states like rectilinear or diagonal. The characteristic of quantum physics states that a state cannot be measured without discarding or disturbing it, which is the central feature of the strength of the quantum cryptographic key (no-cloning theorem).

BB84 key generation depends on two phases: Transmission and Negotiation.
Transmission Phase:

- Alice chooses a bit and a quantum basis (rectilinear or diagonal) to encode her bit
- Bob does not know which basis was used, so he picks his own random measurement basis
- After measurement, he records the result and the basis used

Negotiation Phase:

- Key Sifting: The bases are compared for each bit, and only those bits are kept where the same basis has been used. The rest of the bits are discarded. This forms the Raw Key.
- Eavesdropping Detection: A small portion of the raw key is compared randomly, and if the error rate is above a threshold, the key is discarded and the process is restarted.
- Error Correction: This consists of dividing the raw key into blocks of bits, computing the parity bits, and parity comparison.
- Privacy Amplification: The final stage applied to minimize the number of bits an attacker might know. A shrinking method is applied to their qubits sequence such that the authentication cost is reduced as well as the attacker presence.

Satellite-Based QKD: The Micius Satellite

One of the most significant breakthroughs in making QKD feasible, specifically over long distances, is China's Micius Satellite [11]. While transfer through optical fibers or air causes quantum photons to degrade rapidly, through the vacuum of space, you are able to avoid all the problems associated with losses due to optical fibers.

The satellite aimed to do exactly this and with a distance record of 1203km, it achieved its goal via the transmission of an entangled photon pair to the two receiving stations in Delingha and Lijiang. A light-altering crystal was used to emit entangled photons so that the polarization states would be opposite. The pairs were split and it was found that the photon polarizations were found to be opposite far more than expected, confirming "Spooky Action at a Distance."

Initially, the satellite itself came to be a weak point as it "knew" the sequences of photons and the combined key for decryption. To overcome this, the scientists ensured that the Micius would not "know" anything, and rather than acting as a communications relay it would instead only be relied upon to simply transmit the secret keys.

VI. Quantum Materials For Computing Applications

Overview

In a broader sense, quantum materials are those substances and systems which cannot be explained by semiclassical physics or low-level quantum mechanics. Their properties arise from quantum effects. With the advent of quantum computing systems that are practical, quantum materials that are able to support coherent quantum states and maintain stability for computational operations are crucial. This section intends to explore the current landscape of the choices available and which of these achieve the performance metrics of stability and coherence, as well as gate fidelities.

Superconductors

As of today, superconductors are perhaps the most mature platforms available for quantum computing [12, 13]. Materials such as aluminum, niobium, and tantalum form the backbone of current quantum chips. They have been used by Google's Sycamore and by the Eagle Quantum Computer by IBM.

Superconducting takes place when certain materials, cooled below a certain temperature, are able to exhibit zero electrical resistance and expel magnetic fields. Persistent electric currents can be created without any energy loss via the formation of Cooper Pairs. This property emerges from a quantum phase transition where the material's electrons condense into a coherent quantum state described by a macroscopic wave function. Superconductors are also able to show the Meissner effect, completely excluding magnetic fields from their interior.

Transmon Qubits: Transmon qubits are a popular variety of superconducting qubits, which use Josephson Junctions [13]. Josephson Junctions consist of two superconducting electrodes separated by a thin insulating barrier to exploit quantum tunneling and allow Cooper Pairs to tunnel across the insulating barrier without breaking, thereby maintaining their superconducting properties. This creates the non-linear relationship between current and voltage, which is governed by Josephson equations.

These junctions enable the creation of qubits by providing the anharmonicity needed to isolate specific energy levels and the correct transitions for quantum information processing. Transmon qubits consist of a large capacitor as well, which is connected to a Josephson Junction, which helps make the qubit insensitive to noise.

Topological Insulators

Topological Insulators represent a shift in quantum material design by offering intrinsic protection against certain types of decoherence due to their topological properties [14, 15]. Bismuth Telluride (Bi_2Te_3) and Bismuth Selenide (Bi_2Se_3) provide conducting surface states that are protected by time-reversal symmetry [14].

This enables the realization of Majorana Fermions: a fermion that is its own antiparticle and is inherently resistant to noise [14]. The topological protection arises from the global properties of the electronic wavefunction, that makes this system inherently robust against local perturbations that cause decoherence.

Challenges:

- Experimental verification of true Majorana modes remains contentious
- Topological insulators require precise control over composition, doping, and interface properties
- Surface oxidation and chemical instability may plague such systems

Two-Dimensional Topological Insulators: The field has expanded to include two-dimensional topological insulators, offering unprecedented control over electronic properties through electrostatic gating. Via Van der Waals heterostructure engineering, it is possible to stack different 2D materials, allowing researchers to combine complementary materials such as magnetic materials, superconductors, or ferroelectrics.

VII. Quantum Homomorphic Encryption

Classical Homomorphic Encryption Background

Classical homomorphic encryption (HE) establishes the cryptographic foundation where computations execute on encrypted data without requiring decryption, fundamentally preserving privacy during outsourced processing [16, 17, 18]. However, as quantum computing threatens traditional cryptographic assumptions (such as through Shor's algorithm), quantum homomorphic encryption (QHE) emerges as the natural evolution, extending privacy-preserving computation to quantum data and circuits.

Classical HE schemes are categorized based on the types and number of operations supported:

Partially Homomorphic Encryption (PHE): These schemes allow an unlimited number of operations of only a single type, either addition or multiplication, on encrypted values. A prominent example is RSA, which is partially homomorphic with respect to multiplication.

Somewhat Homomorphic Encryption (SHE): SHE schemes support both addition and multiplication operations, but with a limitation on the number of times these operations can be performed.

Fully Homomorphic Encryption (FHE): FHE is the most versatile type, enabling both addition and multiplication operations with no limit on their number or circuit depth, allowing for arbitrary computations on encrypted data.

Quantum Homomorphic Encryption Principles

Quantum homomorphic encryption extends the concepts of HE into the quantum world, allowing encryption on quantum data without requiring decryption [19]. It operates on three foundational cryptographic principles:

- Quantum one-way functions derive computational security from quantum-resistant mathematical problems, including code-based cryptography rooted in the hardness of decoding random linear error-correcting codes [20].
- The no-cloning theorem ensures encrypted quantum states cannot be duplicated, preventing eavesdropping and unauthorized access to sensitive quantum information.

- Gate teleportation enables homomorphic evaluation through measurement-based quantum computation—where quantum gates are applied via entangled resource states and adaptive measurements—altering how quantum operations are performed on encrypted data.

The EPR Scheme

A prominent example is the "EPR" scheme proposed by Broadbent and Jeffery, which is homomorphic for the universal Clifford+T gate set [21]. This scheme leverages a combination of quantum one-time pads (QOTP) and classical homomorphic encryption, demonstrating a hybrid approach where classical homomorphic encryption is nested within a quantum homomorphic scheme.

Encryption

Key Generation: The client initiates the process by generating a public key (pk) and a secret key (sk) using a classical Fully Homomorphic Encryption (HE) scheme, such as BFV. If the quantum circuit contains L T-gates, the client may need L+1 independent classical homomorphic key sets.

Qubit Encryption (QOTP): For each input qubit |ψ⟩, the client generates a pair of randomly selected secret key bits (a, b). These bits are used to apply a quantum one-time pad (QOTP) to the qubit, transforming it into the state X^a Z^b |ψ⟩, where X and Z are Pauli matrices. This operation makes the encrypted qubit appear as a maximally mixed state to anyone without the key.

Classical Key Encryption: The client then encrypts these classical QOTP keys (a, b) using the classical HE public key (pk), resulting in encrypted keys (ã, b̃). This nesting of classical HE within the quantum scheme reveals that QHE is not purely quantum; it relies on established classical techniques for managing the classical control and key information associated with quantum operations.

Data Transmission: The client sends the encrypted quantum states |ψ̃⟩ along with the classically encrypted QOTP keys (ã, b̃) to the quantum cloud server.

Evaluation

The server receives the encrypted data and the quantum circuit C to be evaluated. The circuit is typically decomposed into universal quantum gates, such as those from the Clifford+T gate set ({X, Z, H, P, CNOT, T}). Before evaluating the circuit, the server appends R EPR pairs to the input of the computation, where R is the total number of T in Circuit. SWAP gates are applied to arrange wires associated with EPR pairs for T-gates adjacent to their corresponding qubits. The server applies the quantum circuit layer by layer, performing operations on the encrypted states and updating the encrypted keys homomorphically.

For Clifford gates (I, X, Z, H, P, CNOT), applying the gate to an encrypted qubit X^a Z^b |ψ⟩ results in a new encrypted state X^a' Z^b' C|ψ⟩. The key update rule (a, b) → (a', b') is a classical operation. The server performs these updates directly on the classically encrypted keys (ã, b̃) using the classical HE scheme. For example, a Hadamard (H) gate swaps the a and b keys (i.e., (a, b) → (b, a)), while a CNOT gate modifies both control and target keys based on a specific rule. The T-gate, on the other hand, is non-Clifford, and its application introduces an additional phase gate dependent on the a key (T X^a Z^b = X^a Z^(a⊕b) P^a T). The intricate "gadget" mechanism and symbolic computation required for T-gates demonstrate that non-Clifford gates pose a disproportionate complexity burden in QHE, driving much of the scheme's design and computational overhead. To correct this, the EPR scheme employs a "T-gate gadget" that utilizes an entangled EPR pair shared between the client and server.

Decryption

After the circuit evaluation, the server returns the quantum state and the modified encrypted keys to the client. The client uses the classical secret key (sk) to decrypt the final encrypted QOTP keys (ã, b̃) and the encrypted bits in M̃ and P̃. If T-gates were involved, decryption proceeds in the order specified by the T list. For each T-gate, the client performs conditional phase gate corrections. After processing all T-gates, the client performs a final classical bit correction procedure to obtain the fully corrected a and b values for the QOTP. The client traces out unnecessary wires (those associated with EPR pairs) and then applies the quantum one-time pad using the corrected a and b values to retrieve the decrypted quantum state.

Noise: Quantum systems are inherently susceptible to noise, decoherence, and gate errors, which pose significant challenges for maintaining computational accuracy in quantum homomorphic encryption (QHE) [22, 23]. One solution is Quantum Error Correction Codes. The integration of QECCs with QHE schemes is considered essential for achieving fault-tolerant secure cloud quantum computing. QECCs protect quantum information from noise by encoding it redundantly across multiple physical qubits. A significant challenge lies in the "significant overheads associated with these schemes," as they typically require substantial resources for encoding and decoding.

Both classical FHE and QFHE face noise accumulation, and "bootstrapping" is a technique used to manage this noise growth. This process "refreshes" ciphertexts when noise becomes too large, allowing for arbitrary numbers of additions and multiplications without excessive noise accumulation. Efficient quantum bootstrapping or alternative noise-reduction techniques remain an elusive goal.

Reliance on Lattice-Based Problems: The Learning With Errors (LWE) problem and its ring variant (RLWE) have emerged as leading candidates for building quantum-resistant cryptographic primitives [24, 25]. LWE's hardness is equivalent to approximating short vector problems in arbitrary worst-case lattices, for which no efficient quantum algorithm is currently known. This makes LWE-based schemes a "gold standard" for security against quantum adversaries. This prevalence indicates a consensus on LWE's perceived strength against quantum attacks, bridging the security requirements of both classical and quantum homomorphic encryption in the post-quantum landscape.

VIII. Conclusion

Quantum cryptography has emerged as one of the most important fields in the past 50 years, combining multidisciplinary research spanning quantum physics, materials science, cryptography, and computer science. Shor's algorithm has had a considerable impact on the world of cryptography, prompting the shift away from computational security and computational assumptions toward information-theoretic security.

The shift to lattice-based problems, where hardness is equivalent to short vector approximations of lattices, provides a foundation for post-quantum cryptographic systems. Research into quantum sensing has produced sensors with multifaceted applications, including quantum cryptography enhancement. Quantum communication protocols, particularly satellite-based QKD systems, have demonstrated practical feasibility for secure global communications.

The exploration of quantum materials reveals significant potential in both superconducting systems and emerging topological conductors. New research on topological conductors suggests untapped potential for scalability improvements. Quantum homomorphic encryption demonstrates the possibility of privacy preservation even during outsourced processing of quantum data.

Overall, while quantum computing and quantum cryptography show tremendous promise, their practical feasibility is prominently hindered by noise and decoherence challenges. Continued research in error correction, materials science, and protocol optimization will be essential for realizing the full potential of quantum cryptographic systems.

References

[1] Shor, Peter W. "Polynomial-Time Algorithms For Prime Factorization And Discrete Logarithms On A Quantum Computer." Arxiv.Org, 1995, Arxiv:Quant-Ph/9508027.

[2] Ekert, Artur, And Richard Jozsa. "Quantum Computation And Shor's Algorithm." Physica D: Nonlinear Phenomena, Vol. 120, No. 1-2, 1998, Pp. 3-33. Sciencedirect, Doi:10.1016/S0378-4371(97)00554-2.

[3] "Post-Quantum Cryptography." Arxiv.Org, 2025, Arxiv:2502.12252. .

[4] "Lecture 4: Quantum Gates And Quantum Circuits." Max Planck Institute For The Science Of Light, 2012. MPL.MPG.DE, Mpl.Mpg.De/Fileadmin/User_Upload/Chekhova_Research_Group/Lecture_4_12.Pdf.

[5] Divincenzo, David P. "The Physical Implementation Of Quantum Computation." Reviews Of Modern Physics, Vol. 79, No. 3, 2007, Pp. 1027-34. Yale University, Boulderschool.Yale.Edu/Sites/Default/Files/Files/Rmp-3-27-08.Pdf.

[6] "Quantum Sensing For Cryptography Enhancement." Arxiv.Org, 2024, Arxiv:2403.19299v1. .

[7] Rosenband, T., Et Al. "Frequency Ratio Of Al+ And Hg+ Single-Ion Optical Clocks; Metrology At The 10^-17 Level." Nature Physics, Vol. 4, No. 1, 2008, Pp. 629-33. Nature, Doi:10.1038/Nphys629.

[8] Maze, J. R., Et Al. "Nanoscale Magnetic Sensing With An Individual Electronic Spin In Diamond." Nature Physics, Vol. 5, No. 9, 2009, Pp. 640-44. Springerlink, Doi:10.1038/Nphys1367.

[9] Yati, Maneesh. "Quantum Cryptography." Researchgate, 2020. Researchgate, Www.Researchgate.Net/Profile/Maneesh-Yati/Publication/345675328_Quantum_Cryptography/Links/5faa8d2e92851cc286a50705/Quantum-Cryptography.Pdf.

[10] "Quantum Key Distribution: BB84 Protocol." Sciencedirect, 2015. Sciencedirect, Doi:10.1016/S1877-0509(15)02844-6.

[11] Yin, J., Et Al. "Entanglement-Based Secure Quantum Cryptography Over 1,120 Kilometres." Nature, Vol. 582, 2020, Pp. 501–505. Nature, Doi:10.1038/S41586-020-2401-Y.

[12] Plourde, B. L. T., Et Al. "Scalable Quantum Computation With Superconducting Circuits." Physical Review Letters, Vol. 128, No. 18, 2022, P. 180502. APS Journals, Doi:10.1103/Physrevlett.128.180502.

[13] Kjaergaard, M., Et Al. "Superconducting Qubits: Current State And Future Perspectives." Arxiv.Org, 2019, Arxiv:1906.01645. .

[14] Murakami, Shuichi, Et Al. "Topological Insulators With Strong Spin-Orbit Coupling." Physical Review B, Vol. 97, No. 6, 2018, P. 060508. APS Journals, Doi:10.1103/Physrevb.97.060508.

[15] Zhang, X., Et Al. "Recent Advances In 2D Topological Insulators." Chemical Reviews, Vol. 121, No. 11, 2021, Pp. 6745-802. ACS Publications, Doi:10.1021/Acs.Chemrev.0c01322.

[16] Gentry, Craig. "Fully Homomorphic Encryption Using Ideal Lattices." Proceedings Of The 41st Annual ACM Symposium On Theory Of Computing, 2009, Pp. 169-78. Wiley Online Library, Doi:10.1002/Spe.3039.

[17] "What Is Homomorphic Encryption?" IEEE Digital Privacy, 2023. IEEE Digital Privacy, Digitalprivacy.Ieee.Org/Publications/Topics/What-Is-Homomorphic-Encryption/.

[18] Goldwasser, Shafi. "Fully Homomorphic Encryption." MIT CSAIL, 2024. MIT CSAIL, 65610.Csail.Mit.Edu/2024/Lec/L08-Fhe.Pdf.

[19] "Quantum Homomorphic Encryption: A Survey." Arxiv.Org, 2023, Arxiv:2305.05904.

[20] "Classical Homomorphic Encryption For Quantum Circuits." Researchgate, 2017. Researchgate,

Www.Researchgate.Net/Publication/318981711_Classical_Homomorphic_Encryption_For_Quantum_Circuits.

[21] Broadbent, Anne, And Stacey Jeffery. "Quantum Homomorphic Encryption For Circuits Of Clifford And T Gates." Arxiv.Org, 2014, Arxiv:1412.8766. .

[22] "Quantum Error Correction." Arxiv.Org, 2024, Arxiv:2401.02128.

[23] "Fault-Tolerant Quantum Computing." Arxiv.Org, 2024, Arxiv:2404.08342.

[24] "Lattice-Based Cryptography." IACR Eprint Archive, 2018, Eprint.Iacr.Org/2018/338.Pdf.

[25] "Post-Quantum Cryptography: Lattice-Based Schemes." Arxiv.Org, 2025, Arxiv:2504.16091.