

Quantum computing: A taxonomy, systematic review and future directions

Sukhpal Singh Gill¹ | Adarsh Kumar² | Harvinder Singh³ | Manmeet Singh^{4,5} | Kamalpreet Kaur⁶ | Muhammad Usman⁷ | Rajkumar Buyya⁸

¹School of Electronic Engineering and Computer Science, Queen Mary University of London, London, UK

²Department of Systemics, School of Computer Science, University of Petroleum and Energy Studies, Dehradun, India

³Department of Virtualization, School of Computer Science, University of Petroleum and Energy Studies, Dehradun, India

⁴Jackson School of Geosciences, University of Texas at Austin, Austin, Texas, USA

⁵Centre for Climate Change Research, Indian Institute of Tropical Meteorology (IITM), Pune, India

⁶Seneca International Academy, Seneca, Toronto, Ontario, Canada

⁷School of Computing and Information Systems, The University of Melbourne, Parkville, Victoria, Australia

⁸Cloud Computing and Distributed Systems (CLOUDS) Laboratory, School of Computing and Information Systems,

Abstract

Quantum computing (QC) is an emerging paradigm with the potential to offer significant computational advantage over conventional classical computing by exploiting quantum-mechanical principles such as entanglement and superposition. It is anticipated that this computational advantage of QC will help to solve many complex and computationally intractable problems in several application domains such as drug design, data science, clean energy, finance, industrial chemical development, secure communications, and quantum chemistry. In recent years, tremendous progress in both quantum hardware development and quantum software/algorithm has brought QC much closer to reality. Indeed, the demonstration of quantum supremacy marks a significant milestone in the Noisy Intermediate Scale Quantum (NISQ) era—the next logical step being the quantum advantage whereby quantum computers solve a real-world problem much more efficiently than classical computing. As the quantum devices are expected to steadily scale up in the next few years, quantum decoherence and qubit interconnectivity are two of the major challenges to achieve quantum advantage in the NISQ era. QC is a highly topical and fast-moving field of research with significant ongoing progress in all facets. A systematic review of the existing literature on QC will be invaluable to understand the state-of-the-art of this emerging field and identify open challenges for the QC community

Abbreviations: ABC, simple matrix scheme or ABC in short; AKCN, asymmetric key consensus with noise; BB84, quantum key distribution scheme; Bi-GISIS, bilateral generalization inhomogeneous short integer solution; CHP, CNOT-hadamard-phase—Scott Aaronson; CK+, extended Cohn-Kanade (CK+) database; Cirq, software library for writing, manipulating, and optimizing quantum circuits; DWDM, dense wavelength division multiplexing; EFC, extension field cancelation; EMBLEM, error-blocked multi-bit LWE-based encapsulation; EQCS, Egyptian Quantum Computing Society; GeMSS, Great Multivariate Short Signature; HFE, hidden field equation; ILWE, integer module learning with errors; KCL, key consensus from lattice; LanQ, a quantum imperative programming language; LDPC, low-density parity-check; LUOV, UOV + PRNG + Field Lifting + Simplified Secret Key; MDPC, moderate density parity check; MLWE, module learning with errors; MPKC, multivariate public key cryptosystems; MPLWE, middle product learning with errors; MQDSS, MQ (multivariate quadratic) digital signature scheme; NC-Rainbow, non-commutative Rainbow; OKC, optimal key consensus; OKCN, optimally balanced key consensus with noise; PRNG, pseudorandom number generator; R. EMBLEM, ring error-blocked multi-bit LWE-based encapsulation; RLWE, ring learning with errors; RDSS, Rainbow digital signature schemes; R-LRS2, Rainbow low resolution spectrograph 2; SRP, MPKC encryption scheme called SRP; SIS, short integer solution; staq, full-stack quantum processing toolkit written in standard C++; TRMS, tractable rational map signature; TTS, tame transformation signature; QCAD, quantum computer aided design; QPU, quantum processing unit; QCGPU, quantum computing GPU; qchas, a library for implementing quantum algorithms; QC-LDPC, quasi-cyclic low-density parity codes; QC-LRPC, quasi-cyclic low-rank parity-check; QIO, quantum input output; QMDD, quantum multiple-valued decision diagram; QOCS, qualified one-way costs shifting; QuEST, Quantum Exact Simulation Toolkit; UOV, unbalanced oil and vinegar.

The University of Melbourne, Parkville,
Victoria, Australia

Correspondence

Adarsh Kumar, Department of Systemics,
School of Computer Science, University of
Petroleum and Energy Studies, Dehradun,
Uttarakhand 248007, India.

Email: adarsh.kumar@ddn.upes.ac.in

to address in the coming years. This article presents a comprehensive review of QC literature and proposes taxonomy of QC. The proposed taxonomy is used to map various related studies to identify the research gaps. A detailed overview of quantum software tools and technologies, post-quantum cryptography, and quantum computer hardware development captures the current state-of-the-art in the respective areas. The article identifies and highlights various open challenges and promising future directions for research and innovation in QC.

KEYWORDS

conceptual model, future directions, methodical analysis, quantum computing, qubits, research challenges, taxonomy

1 | INTRODUCTION

In his famous lecture in 1982, Richard Feynman envisioned a quantum machine working on the laws of quantum mechanics which can simulate quantum physics, and in many ways, this is considered one of the initial conceptions of quantum computing (QC).¹ He postulated that nature is not classical and therefore to simulate natural phenomena, one would need a computing device which works on quantum mechanical principles. Indeed, quantum computers offer such possibilities, where computing can exploit quantum mechanical properties such as entanglement and superposition to offer tremendous computational capabilities necessary for simulations of complex quantum systems. The initial progress toward developing quantum computer hardware was relatively slow, because the proposed quantum mechanical properties are only observed at the very fundamental scale of nature (e.g., electron spins or photon polarization), which were very challenging to manipulate due to technological limitations. However, in recent years, the field of QC has rapidly progressed and emerged as one of the highly topical areas of research. QC has the potential to offer computational capabilities which will surpass existing supercomputers, and this has sparked huge interest from both industry and academia to build a world's first quantum machine. Today, many big companies such as IBM, Google, Microsoft, and Intel, as well as many ambitious start-up companies such as Rigetti and IonQ are actively perusing the race to develop a first large scale universal quantum computer. In parallel to quantum hardware development, the area of quantum software and quantum algorithm development has also seen tremendous progress in the last few years.

It is well known that in conventional classical digital computing, the information is stored and processed as bits which can take a definite binary value ("0" or "1"). The equivalent in QC is known as quantum bit, or just qubit, which by the virtue of quantum mechanics could take values of "0," "1," or any superpositions of "0" and "1" (effectively being in both 0 and 1 states at once!). Quantum computers, therefore, can access an exponentially large Hilbert space (or computational space), where " n " qubits could be in a superposition state of 2^n possible outcomes at any given time. This will allow quantum computers to tackle large scale space problems.

Developing a large-scale quantum computer has its own challenges. One of the major challenges in quantum hardware development arises from decoherence of qubits, whereby qubits lose their coherent properties via interaction with an environment. This implies that qubits in a superposition state will decohere to classical bits and therefore any quantum advantage will diminish. In "Noisy Intermediate Scale Quantum" (NISQ), "noisy" mentions the fact that what is happening in the environment would disturb the devices. To exemplify, small changes in temperature, stray electric or magnetic fields can cause the quantum information in the computer to be degraded.^{2,3} Much of the ongoing research efforts in QC are focused on overcoming errors in NISQ devices by developing efficient error correction protocols. A second major challenge is related to connectivity of qubits in today's quantum devices. It is related to relatively sparse connectivity of qubits in today's quantum devices as it becomes non-trivial to map large depth quantum circuits with many two-qubit gates which require inter-qubit interactions via direct couplings.

Despite technical challenges, NISQ quantum computers are already offering glimpses of computational capabilities. The recent demonstration of quantum supremacy by Google team is a significant milestone in the area of QC.⁴

An intense global race is now ongoing to achieve a first QC application which solves a useful real-world problem that is intractable on classical computers—also known as “quantum advantage.” To achieve this feat, a significant progress in both error-corrected quantum hardware and quantum algorithm development will be required in the coming years.

Quantum algorithms are being developed and benchmarked on NISQ devices at a rapid pace. In early 90s, there were only a few notable quantum algorithms such as Grover’s and Shor’s; however today hundreds of new quantum algorithms have been developed.⁵ Among these, one of the most widely used class of quantum algorithms is variation quantum algorithms such as variational quantum eigensolver (VQE)⁶ which are based on a combination of quantum and classical components. VQE algorithms have shown excellent results on NISQ devices for problems in quantum chemistry and quantum machine learning fields. A few other major categories of quantum algorithms include algebraic (such as discrete log or verifying matrix products), search (such as Grover and amplitude amplification), and variational (such as quantum approximate optimization).

The full potential of QC for real-world applications can only be realized when a large-scale fault-tolerant universal quantum computer will be available which requires several years of further development. However, the quantum speed-up on the existing NISQ era devices is already being accessed for prototype applications exhibiting promising results. Among these, variational quantum algorithms and quantum machine learning are two of the most active areas of research for NISQ devices. Quantum machine learning promises to speed up machine learning algorithms for analyzing the classical data. There have already been proposals for quantum principle component analysis, quantum support vector machine and quantum neural network. It is not yet fully established if quantum machine learning would offer superior computational efficiency when compared to classical machine learning implementations; however, recent work has shown promising results.^{7,8} Quantum computers consume less energy, therefore processing data intensive problems by quantum machine learning algorithms can reduce down energy cost, and the dependency on fossil-fuels will decrease.⁹

For the implementation of quantum algorithms on NISQ devices, there are several well-known models such as the quantum circuit model for gate-based universal QC, adiabatic QC or quantum annealing and one-way quantum computer.² Among these, quantum circuit model is considered as the most practical pathway due to the possibility of reprogramming quantum computers based on a target problem. QC does not yet have its own high-level programming language. In the circuit model, the algorithms are processed by constructing quantum circuits which systematically apply available quantum gates or operations to find the desired solution.

Another highly active area of research in the field of QC is post-quantum secure communication. Cryptography is a technique which is used for hiding information from any unintended recipient.¹⁰ Although quantum cryptography exploits quantum properties for sharing a quantum key (known as quantum key distribution or QKD),¹¹ post-quantum cryptography is still based on constructing classical cryptographic algorithms that hard to break by a quantum computer.¹² For post-quantum cryptography, major work is underway in developing many different techniques such as lattice-based, hash-based and code-based cryptography schemes.¹³

QC is a rapidly progressing field of research with major developments happening all over the world toward many different aspects such as hardware development, software/algorithm development, error correction on NISQ devices, and applications. This article will provide a comprehensive and timely report on the recent progress and future directions, which will be beneficial for researchers as well as industry engineers working on a broad range of topics. As shown in Figure 1, QC brings various advantages for the applications, application developers, and several industries by distributing the primary functions.

1.1 | Basics of QC

The fundamental unit of classical computing is a bit, which can have two possible values “0” or “1” in binary format. Contrarily, in QC the basic unit of information is a quantum bit or qubit. Qubits by the virtue of quantum mechanics can have a value of “0,” “1” or both “0” and “1” simultaneously. Therefore, mathematically a qubit can be represented as $a|0\rangle + b|1\rangle$ where a and b are coefficients which allow mixing or superposition of “0” and “1” states. Figure 2 schematically shows the difference between a bit and a qubit in a superposition state.

The superposition of qubits provides access to a very large computational space which can solve many problems with large computational complexity. For example, a 3-bit number at any given time can have a single value from the set of eight possible values {000, 001, 010, 011, 100, 101, 110, 111}. However, a 3-qubit state can be placed in a superposition of all eight

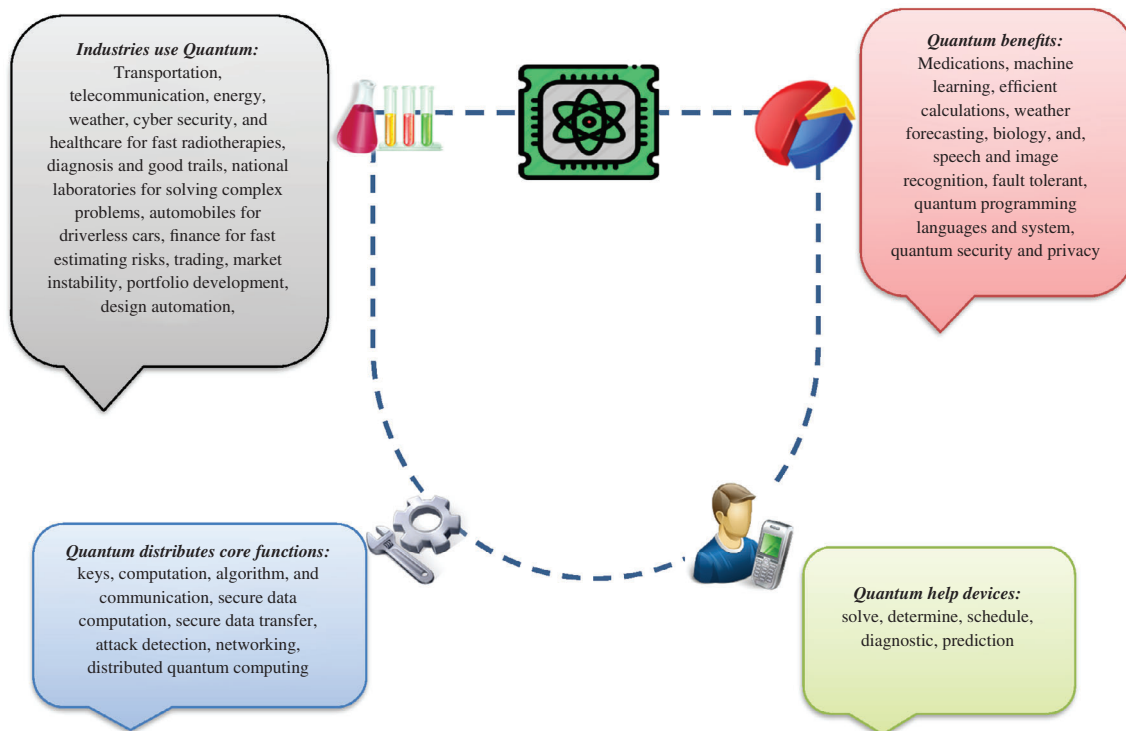


FIGURE 1 Quantum brings various advantages for the applications, application developers, and several industries by distributing the main functions

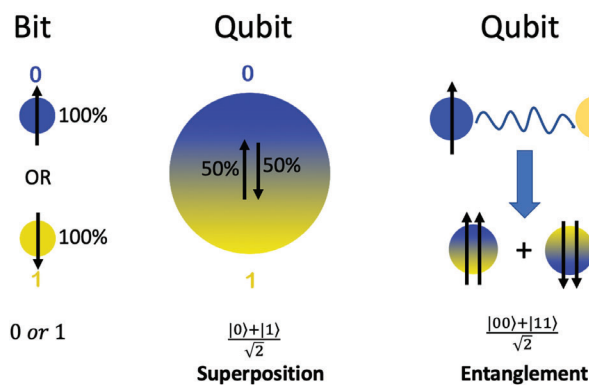


FIGURE 2 Illustration of a bit and qubit. (Left) A bit can take a value of “0” or “1” with 100% probability. (Middle) A qubit can be in a state of $|0\rangle$ or $|1\rangle$ or in a superposition state of both $|0\rangle$ and $|1\rangle$. Here, a qubit is illustrated in a superposition state, composed of 50% $|0\rangle$ and 50% $|1\rangle$. (Right) Illustration of two qubits in an entangled state. The properties of the two qubits in entangled state are linked to each other such that by looking (i.e., measuring) one of them, will reveal the other qubit, even when they are at physically large separations

values: $a|000\rangle + b|001\rangle + c|010\rangle + d|011\rangle + e|100\rangle + f|101\rangle + g|110\rangle + h|111\rangle$. This implies that doubling the number of bits in a classical computing machine will only double the computational space, whereas the same can be achieved by just adding one more qubit, that is, 2^3 to 2^4 by going from 3 to 4 qubits. This exponentially increasing computational space as a function of the number of qubits underpins the power of QC which can handle very large dataset problems with only a small number of qubits. However, the loading of large data sets into quantum states is still an open question. Giovannetti et al.¹⁴ presented the idea of using quantum random access memory, but its implementation on real quantum devices has not been demonstrated yet. Possible other solutions include using coresets constructions¹⁵ and applying machine learning tools for the preparation of quantum states with learned data sets.¹⁶

Another important property of QC is entanglement which is illustrated in Figure 2. In contrast of classical bits where each bit value can be set independent of other bits, qubits can be placed in entangled states. In an entangled state, the properties of qubits are linked to each other, in spite of physical separation between them. Therefore, by measuring one qubit alter the properties of the other qubits which are in the same entangled state. Einstein famously called this “spooky action at distance.” The entanglement is an important resource and can be exploited for dense coding and quantum simulation of correlated systems.

The simulation of a computational problem on a quantum computer typically follows a well-defined set of instructions. This includes the preparation of a superposition state which assigns equal probabilities to all possible outcomes. The implementation of quantum operations exploits superposition and entanglement properties in such a way that the probability of desired outcomes increases whereas the probabilities of other outcomes decrease. The last step in quantum computation is measurement, which leads to collapse of quantum state into the highest probability state providing the desired answer. The implementation of quantum algorithm makes sure that the desired outcome has probability very close to 1, with infinitesimally small probabilities for all other possibilities to achieve high fidelity outcomes.

1.2 | Motivation

The key motivation behind this comprehensive survey is to conduct a review of the existing literature on QC. It covers the definition of QC, its background, taxonomy, comparison of related studies based on taxonomy, quantum software tools and technologies, post-quantum cryptography, and scalable quantum computer hardware. There is a need to identify open challenges and future research directions within the field of QC.

1.3 | Related surveys and our contributions

A few surveys were conducted on QC in the literature. Savchuk and Fesenko¹⁷ presented a general overview of QC research, while Gyongyosi and Imre¹⁸ discussed the fundamentals of quantum mechanics, such as quantum entanglement and quantum superposition. Bruss et al.¹⁹ presented a survey on quantum cryptography until the year 2007 but a lot of advanced research has been carried out in this field after that survey. Abura'ed et al.²⁰ discussed advances in the quantum-theoretical approach to image processing applications only. An introduction to QC for non-physicists was presented by Rieffel and Polak.²¹ Nejatollahi et al.²² proposed a survey on post-quantum lattice-based cryptography implementations, which is just one type of post-quantum cryptography. There is a need for a fresh systematic review which discusses everything from the definition of QC to open challenges. Therefore, this study offers a systematic review of QC literature, its taxonomy and maps the related studies based on this taxonomy. Further, detailed discussion on quantum software tools and technologies, post cryptography and industrial quantum computers is presented along with possible future directions. Table 1 shows the comparison of our survey with the existing surveys.

1.4 | Article structure

The rest of this article is organized as illustrated in Figure 3. Section 2 presents the building blocks and state of the art techniques for QC. The taxonomy of QC and its mapping is proposed in Section 3. Section 4 presents quantum software tools and technologies. The quantum and post-quantum cryptography are presented in Section 5. Section 6 presents the scalable quantum computer hardware. Section 7 highlights the future research directions. Section 8 concludes the article.

2 | BUILDING BLOCKS

Quantum mechanics concepts such as quantum interference, no-cloning theorem, quantum entanglement, and quantum superposition are the underpinning principles of QC. In this section, we review the most recent literature on the technologies related to QC. The QC technologies are anticipated to offer significant speed-up in solving computational

TABLE 1 Comparison of our survey with existing surveys

Survey	General overview	Basics of quantum computing	State of the art techniques	Taxonomy	Quantum cryptography	Mapping of the taxonomy	Quantum software tools and technologies	Post-quantum cryptography	Scalable quantum computer hardware	Future research directions
1	✓ ^a	✓ ^a								
2	✓ ^a	✓ ^a	✓							
3					✓ ^b					
4	✓ ^b	✓ ^b	✓ ^b							
5	✓ ^a									
6								✓ ^b		
7	✓ ^b	✓ ^b	✓ ^a	✓ ^a	✓ ^a	✓ ^a	✓ ^a	✓ ^a	✓ ^a	✓ ^a

Note: 1. Savchuk and Fesenko,¹⁷ 2. Gyongyosi and Imre,¹⁸ 3. Bruss et al.,¹⁹ 4. Abura'ed et al.,²⁰ 5. Rieffel and Polak,²¹ 6. Nejatollahi et al.,²² and 7. Our survey (this article).
^aComprehensive discussion.
^bJust an overview.

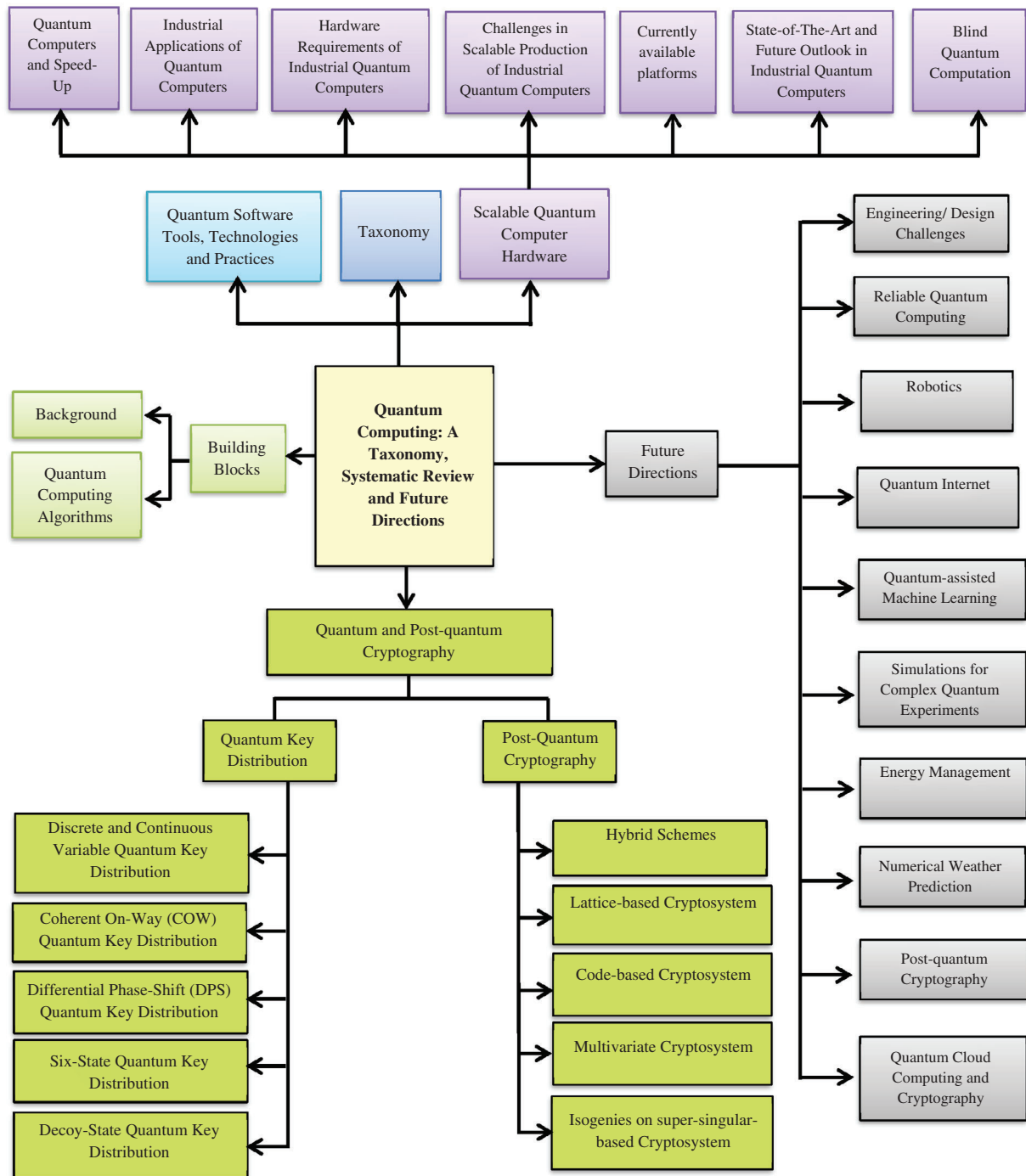


FIGURE 3 The organization of this survey

problems which otherwise are challenging when traditional computing techniques are used. In terms of the size of physical quantum devices, the quantum technologies are still in the phase of incubation.

2.1 | Background

The basic building blocks of a large-scale quantum computer, as shown in Figure 4, consist of a quantum central processing unit, quantum gates, quantum control and measurement circuitry, quantum error detection and correction tools, and quantum memories.

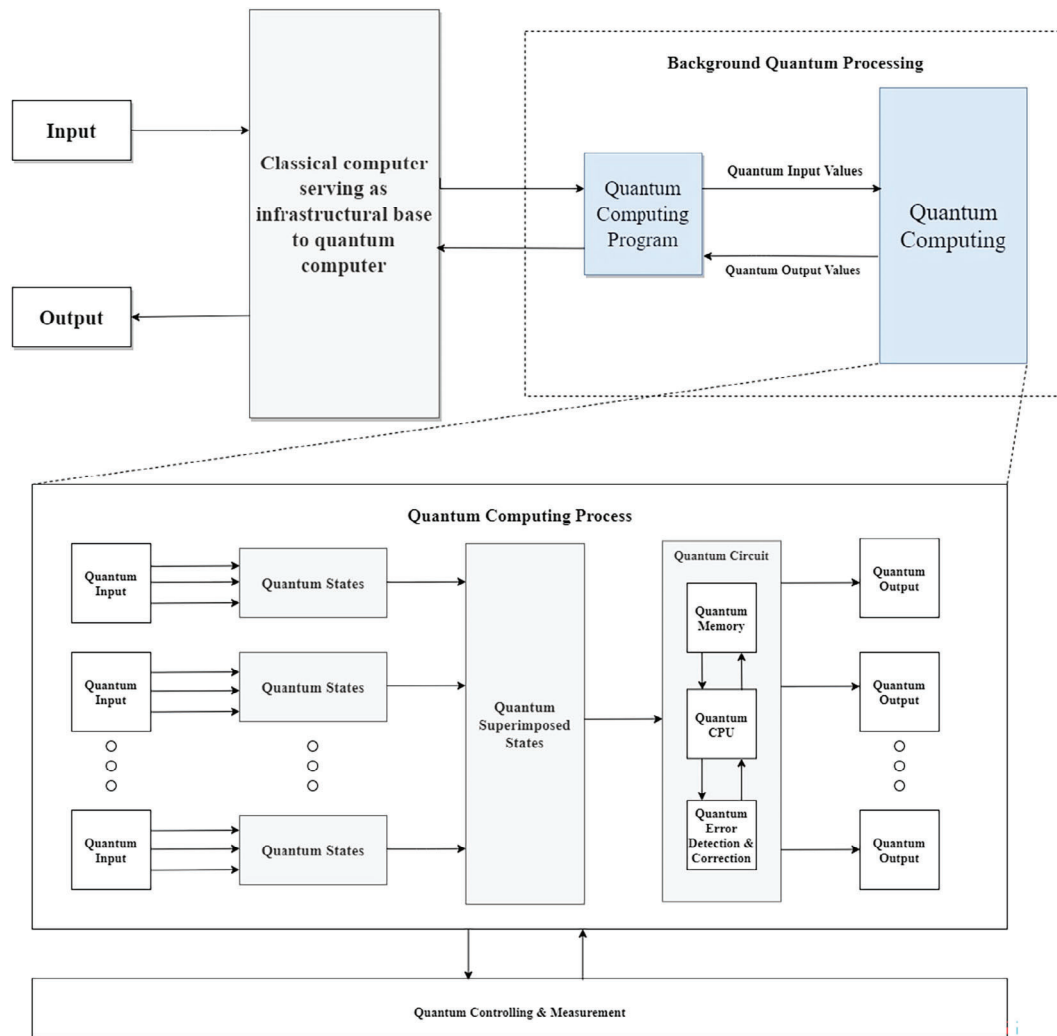


FIGURE 4 Basic building blocks of quantum computers

1. **Quantum gates:** The function of quantum gates in a quantum computer is to perform the operations that are unitary in nature.²³ Quantum gate is a combination of the multiple quantum circuits which uses quantum bits for their operations. Quantum logic gates are reversible in nature. Some examples of quantum gates are identity gate, pauli gates, phase shifter gates, hadamard gates, controlled and uncontrolled gates, rotation operator gates, swap gate, and toffoli gate. All these gates differ in terms of (a) how they are represented, (b) number of qubits they are operating on. Quantum gates can be deployed in various arrangements such as shallow circuits,²⁴ and instantaneous quantum polynomial-time circuit²⁵ depending upon the applications.
2. **Quantum memory:** The collection of multiple quantum states in various superposition arrangements constitutes quantum memories. Quantum memories use quantum registers to save the quantum states of a quantum circuit. Further the quantum states hold the important computational information known as qubits and qutrits. In the recent past, quantum memories have been realized using arrays of quantum states to form a stable quantum system.²⁶
3. **Quantum processing unit:** The quantum processing unit (QPU) is an integral part of the quantum computer which works on the QC principals to accomplish the task. These principles are based on the quantum mechanics, thus there is a significant difference between the conventional central processing unit and the QPU in terms of features. QPU stores the state of computation in terms of quantum mechanical state. It uses the quantum bus for communication among various other units of the quantum computer.²⁷
4. **Quantum control and measurement circuitry:** Quantum control and measurement mechanism is required in quantum computers for the proper monitoring of various manipulations of the quantum states and quantum computations while handling the error correction and detection processes.²⁸

5. Quantum error correction and detection tools: Quantum error detection and correction codes are used to locate and correct the errors that exist during the operations of the quantum gates. Quantum error correction is done to protect the quantum information from the errors that occurred because of quantum noise and decoherence. The error in quantum computers can be identified by using ancilla qubits without disturbing the information in data qubits. It is also important to note that the nature of errors detected in quantum computers is quite different when compared to traditional computing systems because the error can exist due to changes in amplitude or phase of a quantum state.²⁹ Quantum error correction and detection mechanism is required to achieve the fault tolerant quantum computation by not only dealing with the noise on stored quantum information, but also with faulty measurements, faulty quantum measurements and faulty quantum gates.

The core concept of QC such as quantum logic gates, reversible computation idea of Fredkin and Bennet, quantum registers, qubits, Shor's factorization algorithm, quantum complexity, and quantum entanglement has been discussed by Hey³⁰ and Fowler et al.³¹ In the same work, the experimental status has also been reviewed to get a better understanding of the quantum computer's physical implementation. To increase the computing performance of the classical computing system, various architectures of quantum computer that exist in the literature has been explored by Jain.³² The states of the quantum system are fragile in nature. When a quantum system interacts with its surrounding environment, the important quantum information about its states can leak. The leaked information cannot be recovered and used. The progressive deterioration of the state of a quantum system is known as system decoherence. With the existence of decoherence in the quantum system, the assessment of the quantum system will not produce the desired outcomes which can further results in failure of quantum algorithm. The architecture of quantum computer should be such that it should resolve this decoherence problem by proper management of errors that occur when performing quantum arithmetic computations. Kaiser et al. shares the lecture notes targeting those who are beginners to QC field.

The basic idea was to provide the introduction of the fundamental concepts of QC and explain how quantum topology enters the computation field. Buhrman and Rohrig³³ performed a detailed survey of QC techniques and explored its various applications in the distributed network framework. Gyongyosi and Imre¹⁸ reviewed the most recent work done in the field of QC. The experimental results of different QC technologies have been demonstrated, and the problems related to it have been addressed. Savchuk and Fesenko¹⁷ emphasized on the concept of QC which should be scalable. The existing quantum computer has been analyzed in detail for understanding its implementation. Further, it has been concluded that sufficient stress has not been laid by scientists and researchers on developing the scalable quantum computer. Zhang³⁴ explored and revealed the concept of quantum-inspired evolutionary algorithm (QEA) by merging two buzzwords, that is, evolutionary algorithms and QC. The basic architecture and system model of QEA has been explained and reviewed. The comparative analysis of various QEA has been discussed along with future research directions.^{34,35} Han and Kim³⁶ proposed an algorithm that is evolutionary in nature and is inspired by the principles of QEA. The concept of the quantum bits (Q-bit) and quantum gates (Q-gate) have been applied enabling the algorithm to reach out to an optimal solution. For validation of QEA algorithm, its applicability for solving the knapsack problem is demonstrated, and the results have been compared with the traditional genetic algorithm. Rotteler³⁷ provided an overview of quantum algorithms. They stated that quantum algorithms could be classified into three major categories, namely, amplitude amplification type algorithms, hidden subgroup type algorithms, and the quantum algorithm that does not fall in the given two categories as the third category. All the three classifications have been studied to prove how quantum algorithms are different from traditional algorithms and how the computation speed will grow faster by using these quantum algorithms. Li et al.³⁸ discussed merging the elements of quantum mechanics with the intelligent nature-inspired algorithms to mark the new era of computing in the making. Quantum optimization and quantum learning are two classifications based on which the existing quantum algorithms were studied. Further, it was concluded that the nature-inspired quantum algorithms possess high potential when compared with classical-QC algorithms.

For programming a quantum computer, special set of programming language tools are required. Sofge³⁹ analyzed various programming language tools that are present in the market for quantum programmers. They carried out detailed comparative analysis among multiple tools available. Gay⁴⁰ studied and reviewed the concept of quantum programming languages. Further, the design of quantum programming languages including their syntax, semantics and compilers for QC have been discussed, and future research directions have been quoted. Menon and Ritwik⁴¹ pointed out the protocols required to provide the error-free translation of the abilities of the traditional computing system in contrast to the QC system and vice versa. The existing simulators for QC utilizing its capabilities to the fullest extent have been studied.

TABLE 2 Summary of quantum computing algorithms

Name	Year	Type	Objective
Deutsch–Jozsa algorithm ⁴⁶	1992	Based on quantum Fourier transform	Problems requiring exponential queries
Bernstein–Vazirani algorithm ⁴⁷	1992		Efficient solutions of black-box problem
Simon's algorithm ⁴⁸	1994		Faster computation, speedup
Shor's algorithm ⁴⁹	1994		Integer factorization and discrete logarithm problems
Grover's algorithm ⁵⁰	1996	Based on amplitude amplification	Searching unstructured database for marked entry
Quantum counting ⁵¹	1998		Generalized search
Quantum approximate optimization algorithm ⁵²	2014	Hybrid quantum/classical algorithm	Solution of graph theory problems

Kumar et al.⁴² discussed various components of QC like qubits and quantum superposition. Quantum computers have been studied in terms of their efficiency and power. They picked two organizations from the list of organizations dealing with QC and explored for their recent contributions in the field. Further, the research and development challenges related to QC faced by these two organizations have been highlighted as future research challenges. Shaikh and Ali⁴³ demonstrated the significance of big data analytics in QC. Quantum machine learning algorithms that can scale up the processing speed of quantum processors by applying quantum walk in quantum artificial neural networks (ANNs) have been discussed. Yan et al. coined the concept of QIMP, that is, “quantum image processing” which refers to the process of performing all kinds of manipulations on the quantum images for achieving multiple objectives. Further, different QIRs, that is, “quantum image representation” which is the logical representation of the quantum images have been explored, and their applicability has been reviewed.⁴⁴ Roetteler and Svore⁴⁵ stressed on the quantum security mechanisms and protocols involved in the various processes of a quantum computer. The comparative analysis of the cryptographic applications based on the QC system and classical computing system has been done.

2.2 | QC algorithms

Nobel laureate Richard Feynman was the first to postulate the idea of a quantum computer. The properties of quantum mechanics are leveraged by quantum computers and these properties form the basis of quantum computers. The quantum algorithms have come a long way starting from the simulations of quantum physics to a variety of applications in computer science. An industrial scale quantum computer will be a prized progress in achieving the processing power of its kind, which would have implications in various fields such as cybersecurity and others. The first quantum algorithm to find speed greater than that of a classical algorithm was proposed by Daniel Simon. Table 2 shows the comparison of QC algorithms.^{31,49–58}

3 | TAXONOMY

In this section, QC technologies are classified based on different types of features and operations. The various components of the QC taxonomy are (a) basic characteristics, (b) algorithmic characteristics, (c) time and gate characteristics, and (d) other characteristics. A diagrammatic representation of the taxonomy of QC is shown in Figure 5. We share a brief description of every element of QC taxonomy.

- *Basic characteristics:* The basic characteristics of QC include elements like qubit implementation, classification based on QC technology and performance metrics. The basic features of QC are to explore how qubits can be implemented and represented. Qubit representation can be done either in stationary, flying, or mobile ways. The stationary method is similar to traditional programming, whereas mobile approach resembles designing conventional circuits.

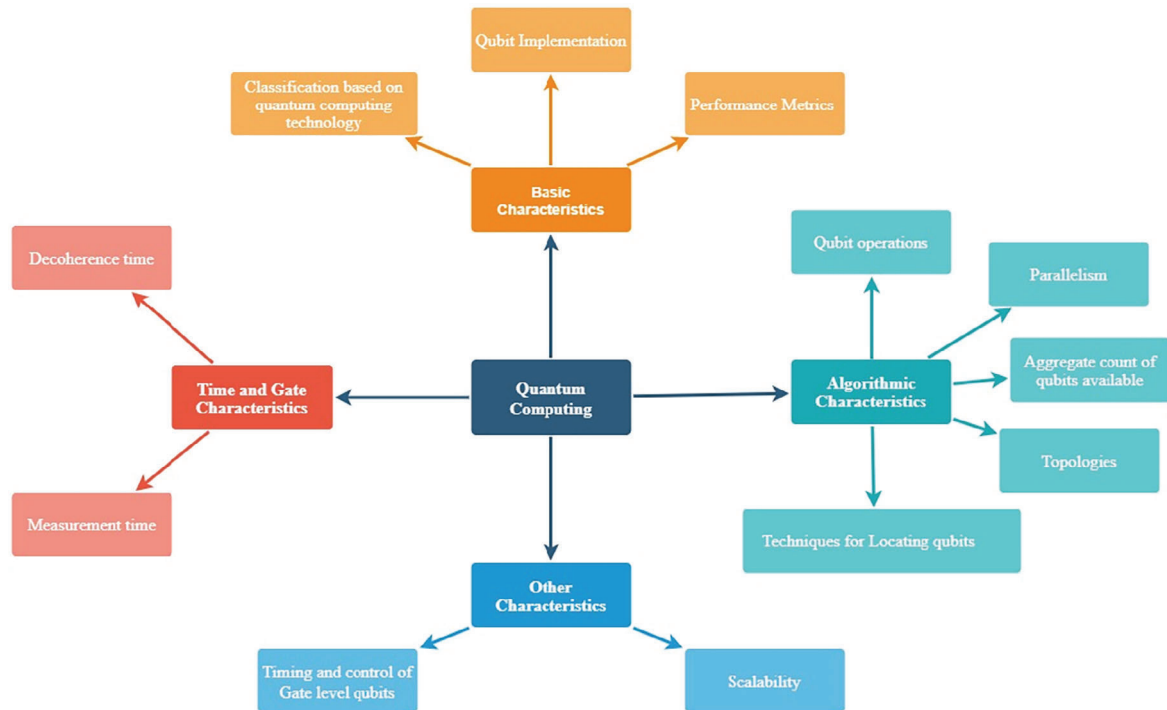


FIGURE 5 Taxonomy of quantum computing technology

Further, the ensemble computing and singleton computing is another classification based on the choice of QC technology. An ensemble computing system is a group of quantum computers that are identical in specifications and performs the same set of functions. In contrast, the singleton computing system consists of a single quantum computer performing designated operations. The performance metrics forms the base of another classification of QC techniques which has mechanical vibrations, fluorescence and concurrency as its attributes.^{41,42}

- Algorithmic characteristics:** QC techniques can be realized by implementing quantum algorithms on the classical computing infrastructure. It is essential to discuss and categorize the QC technologies on the basis of characteristics represented by quantum algorithms. The algorithmic elements of QC technologies include: parallelism, aggregate count of qubits available, topologies, techniques for locating the qubits, and qubit operations. Parallelism is the central feature because the parallel implementation of quantum gates is required to either prevent or minimize the qubits decoherence. The aggregate count of qubits available is another feature that helps in realizing the reliability and scalability of the quantum computer. The various possible arrangements of different physical devices in the architecture of the quantum computer are termed as its topologies. Architecture optimization is the primary concern as it enables the smooth flow of data and information among different physical units of the system. The addressing scheme for locating an individual qubit is logically very complex. This feature enables to explore the qubit states more specifically as far as the quantum computer physical implementation is concerned. Further, for performing any operation on qubits, they have to be moved from the address where they are stored to the location where the qubit gates are performing the action on them.³⁷
- Time and gate characteristics:** The QC technologies can be further classified on the basis of time and gate characteristics which include components such as decoherence time and measurement time. The decoherence time is given by the time until which a qubit can be kept in a specific state. The decoherence time is the topic of research in the field of QC nowadays. Another essential characteristic of classification is the measurement time which is the time required to measure the qubit state precisely.^{7,17}
- Other characteristics:** They include scalability, timing, and control of gate-level qubits on which the classifications of QC technologies have been done. All of the above-discussed features contribute toward the scaling of qubits to larger numbers. Meanwhile, it is recommended to use multiple qubits so that it will not always represent a single ion or photon. The changes in the qubit states are a continuous process with respect to time, hence computing an accurate

TABLE 3 Taxonomies-based mapping of quantum computing techniques

Work	QI	CQCT	PM	P	ACQA	T	TLG	QO	DT	MT	TCGLQ	S
Weitenberg et al. ⁵⁹	✓	✓	✓	✓	✓	×	✓	×	✓	×	✓	✓
Tomza et al. ⁶⁰	✓	✓	✓	✓	✓	✓	✓	×	✓	×	✓	✓
O’Gorman et al. ⁶¹	✓	✓	✓	✓	✓	×	✓	✓	✓	✓	✓	✓
Compagno et al. ⁶²	✓	✓	✓	×	×	×	✓	×	×	×	✓	✓
Schaal et al. ⁶³	✓	✓	✓	×	✓	×	✓	×	×	×	✓	✓
Zwanenburg et al. ⁶⁴	✓	✓	✓	×	✓	×	×	✓	✓	×	✓	✓
Veldhorst et al. ⁶⁵	✓	✓	✓	×	✓	×	×	✓	×	×	✓	✓
Mizuta et al. ⁶⁶	✓	✓	✓	×	✓	×	×	×	×	×	×	×
de Alborno et al. ⁶⁷	✓	✓	✓	×	✓	×	×	✓	×	×	✓	×

Abbreviations: ACQA, aggregate count of qubits available; CQCT, classification based on quantum computing technology; DT, decoherence time; MT, measurement time; P, parallelism; PM, performance metrics; QI, qubit implementation; QO, qubit operations; S, scalability; T, topologies; TCGLQ, timing and control of gate level qubits; TLG, techniques for locating qubits.

timing of gates is critical. The arrival times of the qubits should be precisely adjusted while placing multiple qubits in their relative phases at the same time.^{18,21}

The various QC technologies are categorized based on our proposed taxonomy. The taxonomy-based mapping of QC techniques is shown in Table 3. The QC technologies considered for mapping are chosen based on the following criteria:

1. It represents the most recent and significant research work done in the field of QC.
2. It should exhibit the fundamental characteristics defined in the taxonomy of QC which forms the basis of mapping.

4 | QUANTUM SOFTWARE TOOLS, TECHNOLOGIES, AND PRACTICES

In comparison to the fields of quantum hardware development and quantum simulations, the area of quantum software development is relatively new and less established. Recently quantum software tools are being developed at a rapid pace with many quantum software packages now available from different platforms/sources such as Google, IBM, Microsoft, and D-Wave. These software tools are still at relatively low level such as at the level of assembly language; high-level quantum programming analogous to classical programming tools such as C++ and Java are not yet available.

Table 4 shows the comparative analysis of quantum tools available to-date. The analysis performed in Table 4 presents the current scenario and it may change in future in highly dynamic quantum world and its growth. The parameters used for comparative analysis are briefly explained as follows: (i) a *library* is considered as a collection of functions or classes designed for quantum information and similar computations, (ii) a *tool* is a piece of software that can simulate QC or associated calculations, (iii) the QC libraries, tools, or techniques are found to be either *open-source*, *commercial* or *freeware*, (iv) graphical user interface (*GUI*)-based quantum tools are available that ease the job of circuit designing, programming and displaying the results for users, (v) many GUI-based tools can display the results either in *two or three-dimensions*, (vi) additionally, many tools have *command-line usage* where instructions are predefined to connect the gates, design the inputs and observe the outputs, (vii) *quantum gates* are analogous to conventional logic gates for quantum computers. Few examples of quantum gates include Hadamard, phase shifter, controlled, uncontrolled, and controlled NOT (CNOT) gate. (viii) In this work, a review of most of the quantum programming tools available for academic or research work, used for *simulation* rather than *real-implementation*, is performed (ix) while exploring the quantum tools, it has been observed that many of such tools provide an existing implementation of quantum algorithms. Few of these algorithms include Shor, Deutsch-Jozsa, Simon, quantum phase estimation, hidden subgroup, and Grover algorithms.^{53,57}

TABLE 4 Comparative analysis of software tools and technologies

Tool/technique name	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	Underpinning programming language
QuEST ⁶⁸	✓	✓	✓	×	×	×	×	×	✓	✓	✓	×	×	×	×	C
Staq ⁶⁹	✓	✓	✓	×	×	×	×	×	✓	✓	✓	×	×	×	×	C++
Scaffold/ScaffCC ⁷⁰	✓	✓	✓	×	×	×	×	×	✓	×	✓	×	✓	×	×	Scaffold
Qrack ⁷¹	✓	✓	✓	×	×	×	×	×	✓	×	✓	×	×	×	×	C++
QX Simulator ⁵⁷	✓	✓	✓	×	×	×	×	×	✓	×	✓	×	×	✓	×	Quantum Code
Quantum++ ⁷²	✓	✓	✓	×	×	×	×	×	✓	×	✓	×	×	×	×	C++
QMDD ⁷³	✓	×	✓	×	×	×	×	×	✓	×	✓	×	×	×	✓	C++
CHP ⁷⁴	✓	×	✓	×	×	×	×	×	✓	✓	✓	×	✓	×	×	C
Eqcs ⁷⁵	✓	×	✓	×	×	×	×	×	✓	✓	✓	×	×	×	×	C
LanQ ⁷⁶	✓	×	✓	×	×	×	×	×	✓	✓	✓	×	✓	✓	×	LanQ
libquantum (C) ⁷⁷ / (C++) ⁷⁸	✓	×	✓	×	×	×	×	×	✓	✓	✓	×	✓	✓	×	C, C++
Open Qubit ⁷⁹	✓	×	✓	×	×	×	×	×	✓	✓	✓	×	✓	×	×	C++
Quantum Programming Studio ⁸⁰	×	✓	✓	×	×	×	×	✓	×	✓	✓	×	✓	✓	✓	Javascript
Qubit Workbench ⁸¹	×	✓	×	✓	×	✓	×	✓	×	✓	✓	×	✓	×	✓	–
Linear AI ⁸²	✓	×	×	×	✓	✓	×	×	✓	✓	✓	×	✓	×	✓	Mathematica
QCAD ⁸³	×	✓	×	×	✓	✓	✓	✓	×	✓	✓	×	×	×	✓	–
qsims ⁸⁴	✓	✓	✓	✓	×	×	×	×	✓	✓	✓	×	✓	✓	×	C++
Q-gol ⁸⁵	✓	✓	✓	×	×	✓	✓	✓	×	✓	✓	×	✓	×	×	CaML
QOCS ⁸⁶	✓	✓	✓	×	×	×	×	×	✓	✓	✓	×	✓	×	×	OCaML
Q++ ⁸⁷	✓	×	✓	×	×	×	×	×	✓	✓	✓	×	✓	×	✓	C++
Qinf ⁸⁸	✓	✓	✓	×	×	×	×	×	×	✓	✓	×	×	×	✓	Maxima
Quantum Fog ⁸⁹	✓	✓	✓	×	×	✓	×	✓	×	✓	✓	×	✓	✓	✓	–
SimQubit ⁹⁰	✓	✓	✓	×	×	✓	×	✓	×	✓	✓	×	✓	×	✓	C++
Q-Kit ⁹¹	×	✓	×	×	✓	✓	×	✓	×	✓	✓	×	✓	✓	✓	–
Bloch Sphere ⁹²	✓	✓	✓	×	×	✓	✓	✓	×	✓	✓	×	✓	×	✓	Java
BackupBrain ⁹³	✓	✓	✓	×	×	✓	×	×	×	✓	✓	×	✓	×	✓	Javascript
Quantum Circuit ⁹⁴	✓	✓	✓	×	×	×	×	×	✓	✓	✓	×	✓	×	✓	Javascript
Jsquis ⁹⁵	✓	✓	✓	×	×	×	×	×	✓	✓	✓	×	×	×	×	Javascript
QSWalk.jl ⁹⁶	✓	✓	✓	×	×	✓	×	×	✓	✓	✓	×	×	×	×	Julia
QuantumOptics.jl ⁹⁷	✓	✓	✓	×	×	✓	✓	×	✓	×	✓	×	✓	×	✓	Julia
QuantumWalk.jl ⁹⁸	✓	✓	✓	×	×	✓	×	×	✓	✓	✓	×	✓	×	×	Julia
Feynman ⁹⁹	✓	✓	✓	×	×	✓	×	×	✓	✓	✓	×	✓	✓	×	Maple
OpenQUACS ¹⁰⁰	✓	✓	✓	×	×	✓	×	×	✓	✓	✓	×	✓	✓	×	Maple
Quantavo ¹⁰¹	✓	✓	✓	×	×	×	×	×	✓	✓	✓	×	✓	✓	×	Maple
QDENSITY ¹⁰²	✓	✓	✓	×	×	✓	×	×	✓	✓	✓	×	×	×	✓	Mathematica
Quantum ¹⁰³	✓	✓	×	×	✓	✓	×	×	✓	✓	×	×	✓	✓	✓	Mathematica
QuantumUtils ¹⁰⁴	✓	✓	✓	×	×	×	×	×	✓	✓	✓	×	×	✓	✓	Mathematica
Qi ¹⁰⁵	✓	✓	✓	×	×	×	×	×	✓	✓	✓	✓	×	×	×	Mathematica

(Continues)

TABLE 4 (Continued)

Tool/technique name	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	Underpinning programming language
M-fun ¹⁰⁶	✓	×	✓	×	×	✓	×	×	✓	✓	✓	×	×	×	×	MATLAB/Octave
Quantencomputer ¹⁰⁷	✓	✓	×	×	×	×	×	×	✓	✓	✓	×	✓	×	×	MATLAB
Drqubit ¹⁰⁸	×	×	✓	×	✓	×	×	×	✓	✓	✓	×	×	✓	×	MATLAB
Qubit4Matlab ¹⁰⁹	✓	×	✓	×	×	×	×	×	✓	✓	✓	×	✓	✓	✓	MATLAB
QuIDE ¹¹⁰	×	✓	✓	×	×	✓	×	✓	×	✓	✓	×	✓	✓	✓	.NET
Quantum.NET ¹¹¹	✓	✓	✓	×	×	×	×	×	✓	✓	✓	×	×	×	×	.NET
Qubit Workbench ⁸¹	×	✓	×	×	✓	✓	×	✓	×	✓	✓	×	×	×	×	–
Cirq ¹¹²	✓	✓	✓	×	×	×	×	×	✓	✓	✓	✓	✓	✓	✓	Python
ProjectQ ¹¹³	✓	✓	✓	×	×	×	×	×	✓	✓	✓	×	✓	✓	✓	Python
QCCircuits ¹¹⁴	✓	✓	✓	×	×	×	×	×	✓	✓	✓	×	✓	✓	✓	Python
Qiskit ¹¹⁵	✓	✓	✓	×	×	✓	×	×	✓	✓	✓	✓	✓	✓	✓	Python
OpenQasm ¹¹⁶	✓	✓	✓	×	×	×	×	×	✓	✓	✓	×	×	×	✓	QASM
QCGPU ¹¹⁷	✓	✓	✓	×	×	×	×	×	✓	✓	✓	×	×	✓	×	Rust and OpenCL
QIO ¹¹⁸	✓	×	✓	×	×	×	×	×	✓	✓	✓	×	×	×	✓	Qio + Haskell
Qchas ¹¹⁹	✓	×	✓	×	×	×	×	×	✓	✓	✓	×	×	×	✓	Haskell
Quantum User Interface ¹²⁰	×	✓	✓	×	×	✓	×	✓	×	✓	✓	×	×	×	×	Protobuf
Quantum Development Kit (QDK) ¹²¹	✓	✓	✓	×	×	✓	×	×	✓	✓	✓	×	✓	✓	✓	Python, Q#

Note: A. Library, B. Toolkit, C. Open source, D. Commercial, E. Freeware, F. GUI-based, G. 3D visualization, H. Drag and drop support, I. Command-line usage, J. Support for quantum gates, K. Simulation, L. Real-implementation, M. Built-in quantum algorithm support, N. Gates scheduling and parallelism, O. Diagram or matrix support.

These algorithms are classified in one of the following categories: quantum Fourier transform, amplitude amplification, quantum walks, bounded-error quantum polynomial time (BQP)-complete, and hybrid quantum/classical, (x) gates scheduling, and parallelism is vital for circuit designing that is analogous to quantum computer operations. This concept speed-up the operations in QC, and (xi) most of the quantum gates require matrix operations for their computations. This matrix and associated operations are incorporated in many tools. Table 4 shows the comparative analysis of quantum tools with the above parameters. This comparative analysis shows the programming languages used in the tools as well.

Figure 6 shows the major software engineering practices observed in recent studies of QC world. These practices are briefly explained as follows.^{122–124}

- *Software applications:* In software applications, quantum programming languages, QC-based compilers, QC-based logical level schedulers and optimizers, QC-based error-correction firmwares, QC-based physical level schedulers and optimizers, and QC-based device control firmware are major areas observed in recent studies. Figure 7 shows the classification of software applications in QC.
- *Quantum programming languages:* Various studies are performed to discuss the importance and challenges of quantum programming languages.^{40,125–130} According to Heim et al.¹²⁶ and Gay,⁴⁰ important aspects to study in this domain includes (i) programming language designs (PLD), (ii) programming language semantics (PLS), (iii) programming language compilation (PLC), (iv) commuting operations (CO), (v) controlled operations (COp), adjoint operations (AO), and clean and borrowed qubits (CbQ).^{127–130} The important challenges in quantum programming languages include^{40,125–130}: (i) to program infinite data types in programming languages that ensure storing of infinite quantum-data, (ii) to design quantum concurrency systems that support potential applications, (iii) to provide quantum computation supported virtual machines, (iv) to design algorithms that support customized error correction techniques in programming languages, (v) to focus on programming language designs like imperative, functional, and other languages and λ -calculi, (vi) to apply linear logics in programming languages-based applications, (vii) to apply

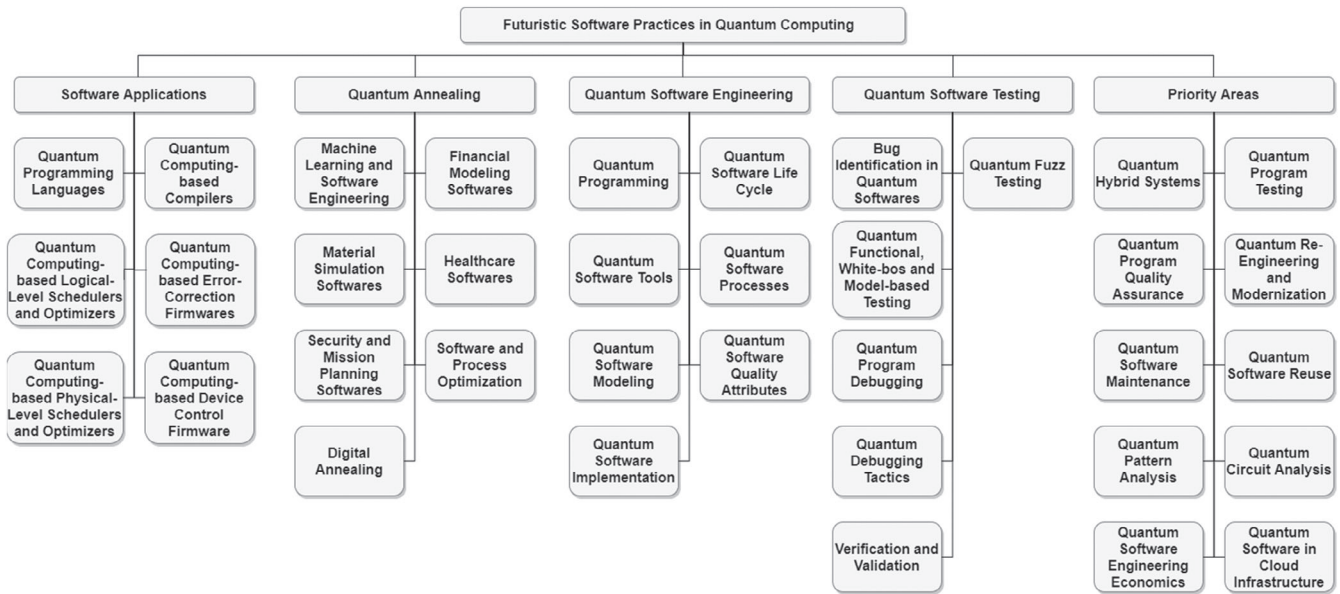


FIGURE 6 Futuristic software practices in quantum computing world

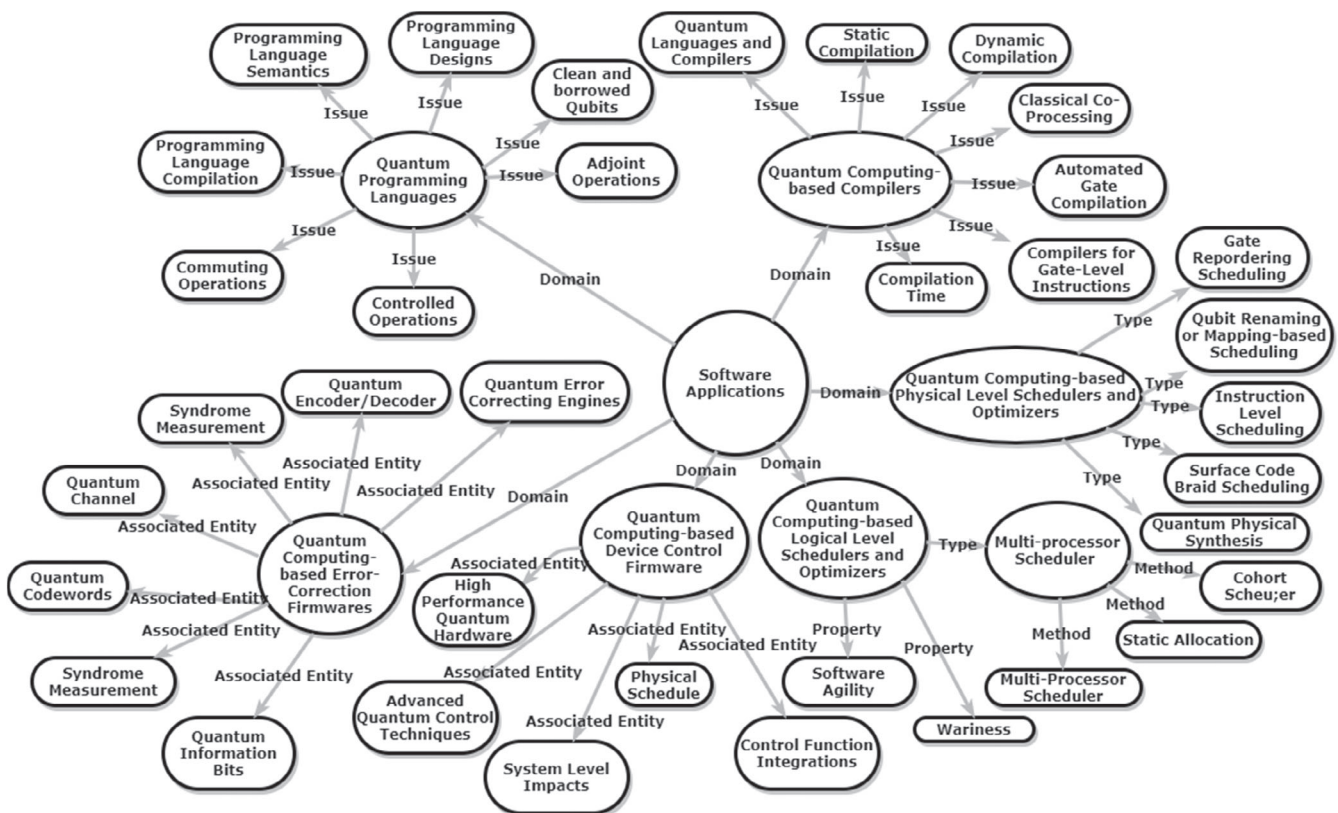


FIGURE 7 Software applications in quantum computing

domain-theoretic semantic techniques in programming languages, and (viii) to explore new semantic techniques in futuristic quantum programming languages.

- **QC-based compilers:** In compilation, the important areas explored in recent studies include (i) quantum languages and compilers (QLC), static compilation (SC), dynamic compilation (DC), classical co-processing (CC), automated gate compilation (AGC), compilers for gate-level instructions (CGLI), and compilation time (CT). According to Chong

et al.,¹³¹ the major challenges in designing QC-based compilers include (i) designing a hybrid system that supports the compilation of algorithms to gate and machine level instructions, (ii) time, memory, and cost-optimized compilation time, (iii) capability to ensure parallelism and optimal scheduling operations for practical scenarios, and (iv) coordinated compilation between quantum and classical processing. In this coordination, classical processing communicates the precision requirements whereas quantum computation communicates the noise and effort information in hybrid systems.

- *QC-based logical level schedulers and optimizers:* In References 132–137, logical scheduling and optimization studies are analyzed in QC-related scenarios. For example, Oskin et al.¹³² discussed the role of dynamic quantum compiler/scheduler in fault-tolerant QC architecture. The processor used in fault-tolerant QC architecture takes logical quantum operations in addition to other control flows and qubit operations. The major challenges in this area include the execution of all quantum algorithms with error correction approaches which make the whole architecture inefficient. Thus, performance optimization, priority-based error measurement, and knowledge of dynamic compilation and algorithm execution should be studied. Likewise, various challenges associated with logical level schedulers and optimizers include (i) integrating the use of multi-processor schedulers and optimizers for error-free quantum physical synthesis, cohort scheduling, and scenarios, where there is a need to apply static compiler/processor allocation, (ii) compilation time, is another important challenge in the quantum world. Thus, applying software agility processes to optimize the job execution with the integration of heavy quantum mechanics (like error-correcting codes with all quantum algorithms) is important to consider, and (iii) lack of trust (wariness) in quantum nodes of quantum network raises concerns over fair and transparent scheduling and optimization jobs. Thus, authentic nodes should be considered to assign the scheduling jobs. Trusted and authentic node identification for scheduling and optimization is important to consider in the future.
- *QC-based physical level schedulers and optimizers:* Physical synthesis, scheduling, and optimization processes are important to reduce the latency in quantum circuits, improve the performances, proper circuit allocation, and efficient sharing of the resources between processes. In this process, the important challenges that need to be addressed include^{138–140}: (i) how to apply proper placement and routing heuristics in physical design layout, (ii) to design effective data flow-based gates or circuit placement and routing. Various students in recent times have explored graph-based data flow approaches to accomplish this task, (iii) to apply proper instruction-level scheduling in instruction issue logic to quantum gates and circuits, (iv) to apply iteration of optimization loops in the scheduling information and incremental updates in scheduling processes, and (v) among other challenges, identification of appropriate heuristic algorithm, error analysis approach, and performance analysis (e.g., time complexity analysis) are required to be studied in future.
- *QC-based error-correction firmwares/software:* An efficient quantum error-correction firmware integrates the quantum algorithms and imperfect hardware efficiently. Error-correcting quantum firmware lies at the lowest level of the QC stack and helps in reducing the error caused by imperfect hardware, its complexity, and resource intensity. In quantum error-correcting codes, the important direction to explore include (i) designing efficient quantum error-correcting engines, (ii) developing high-performance quantum hardware, (iii) apply advanced quantum control techniques to operate the hardware, (iv) effectively handle the quantum information bits in storage, processing, and transmission stages, (v) apply appropriate syndrome measurement approach, (vi) integrating all algorithms with quantum code-words, (vii) to apply an effective quantum error-correcting approach that supports quantum channel (with quantum and classical information processing), (viii) to integrate high-quality error encoder and decoder at two ends of data transmission.
- *QC-based device control firmware:* Software that handles the quantum hardware are expected to provide high performance, ability to apply advanced quantum control techniques, high-quality system-level impacts, simulation-optimization based control for local and global optimum solutions, and appropriate physical schedules.
- *Quantum annealing:* Quantum annealing helps in the identification of the global minimum of a given objective function and set of possible solutions. Quantum annealing is used in various software-based components and applications.^{141–144} Figure 8 shows the usage and associated entities of quantum annealing observed in recent studies. In recent studies,^{141–143} quantum annealing is found to be applied in developing a system that automatically reduces the stress level, factoring the pseudo-random functions, analyzing the cybersecurity data, and other applications including finance and healthcare data analysis.¹⁴⁵ Quantum annealing can be used like simulation annealing to find optimum solutions using well-defined single or multi-objective functions. Thus, can be used to handle various problems like the

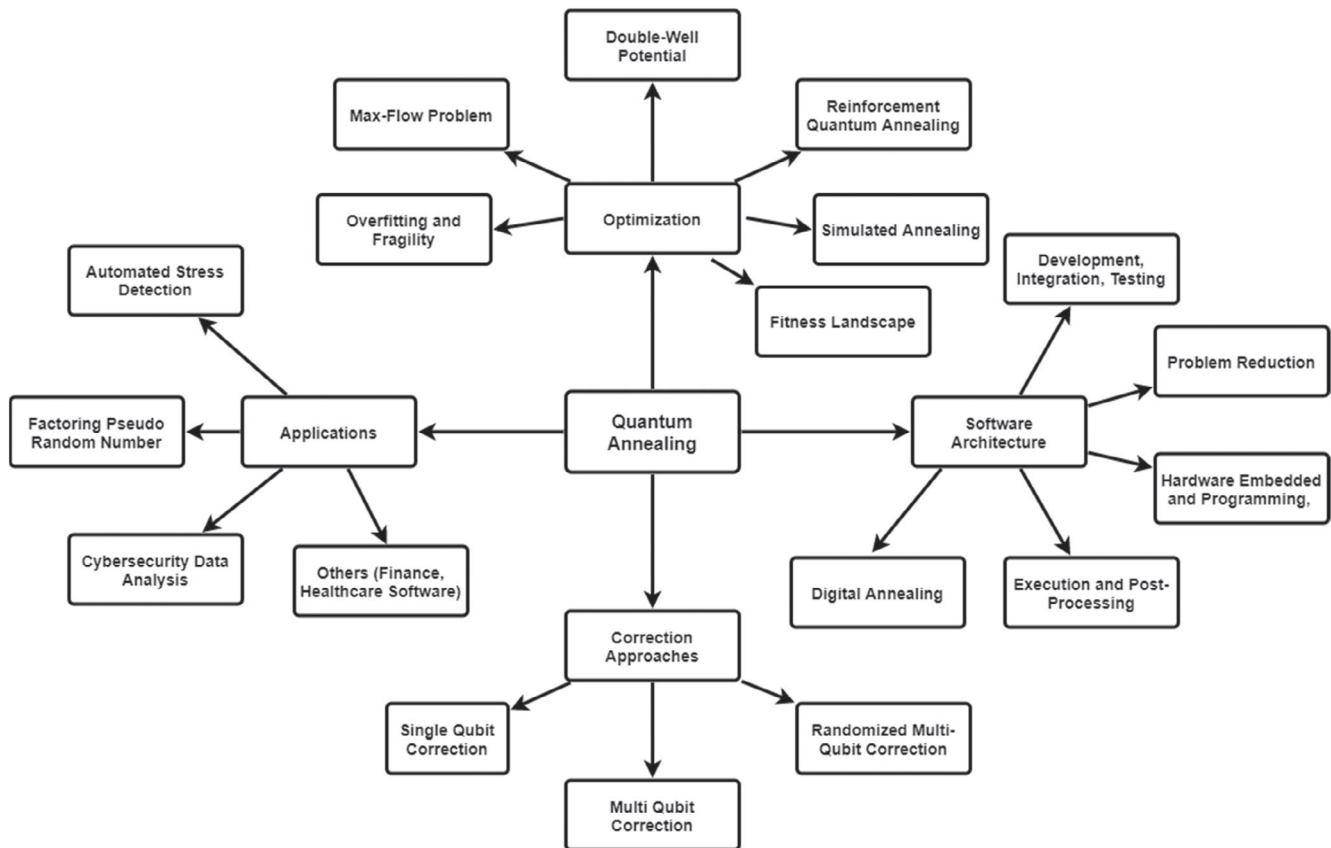


FIGURE 8 Quantum annealing-based software components

Max-Flow problem in a quantum computer.¹⁴⁶ Further, quantum annealing can be used in error correction codes and software architectures to find the global minimum solution in a different set of problems.

- *Quantum software engineering:* In References 122 and 147 recent trends of quantum software engineering are studies. It has been observed that quantum software engineering includes the domain like quantum programming, quantum software tools, quantum software modeling, quantum software implementation, quantum software life cycle, quantum software processes, and quantum software quality attributes. Additionally, this domain studies the syntax and semantics used in programming languages to develop software, quantum, and dynamic logics applied in assertional reasoning to solve challenges in software, characterizing the contract-based disciplines to quantum software.
- *Quantum software testing:* Like classical software testing techniques, quantum software testing also includes various domains like quantum fuzz testing, quantum functional, white-box, and model-based testing, quantum program debugging, quantum debugging tactics, bug identification, and quantum software verification and validation processes.
- *Priority areas:* In QC, certain priority areas are focused largely to make quantum computers and computing a reality. Few examples of such areas include quantum hybrid systems (supporting classical and quantum computation together), quantum program testing (for verifying and validating the program outcomes), quantum program quality assurance, quantum re-engineering and modernization, quantum software maintenance, quantum software reuse, quantum pattern analysis (using quantum artificial intelligence or quantum machines learning), and quantum circuit analysis.
- *Other software dimensions:* In addition to the above-discussed domains, there are a large set of quantum software aspects that can be explored.¹⁴⁸ For example, quantum provenance in the quantum circuit, data analysis, and quantum compilers. Figure 9 shows the various software-related entities in the quantum software life cycle that need exploration in detail.

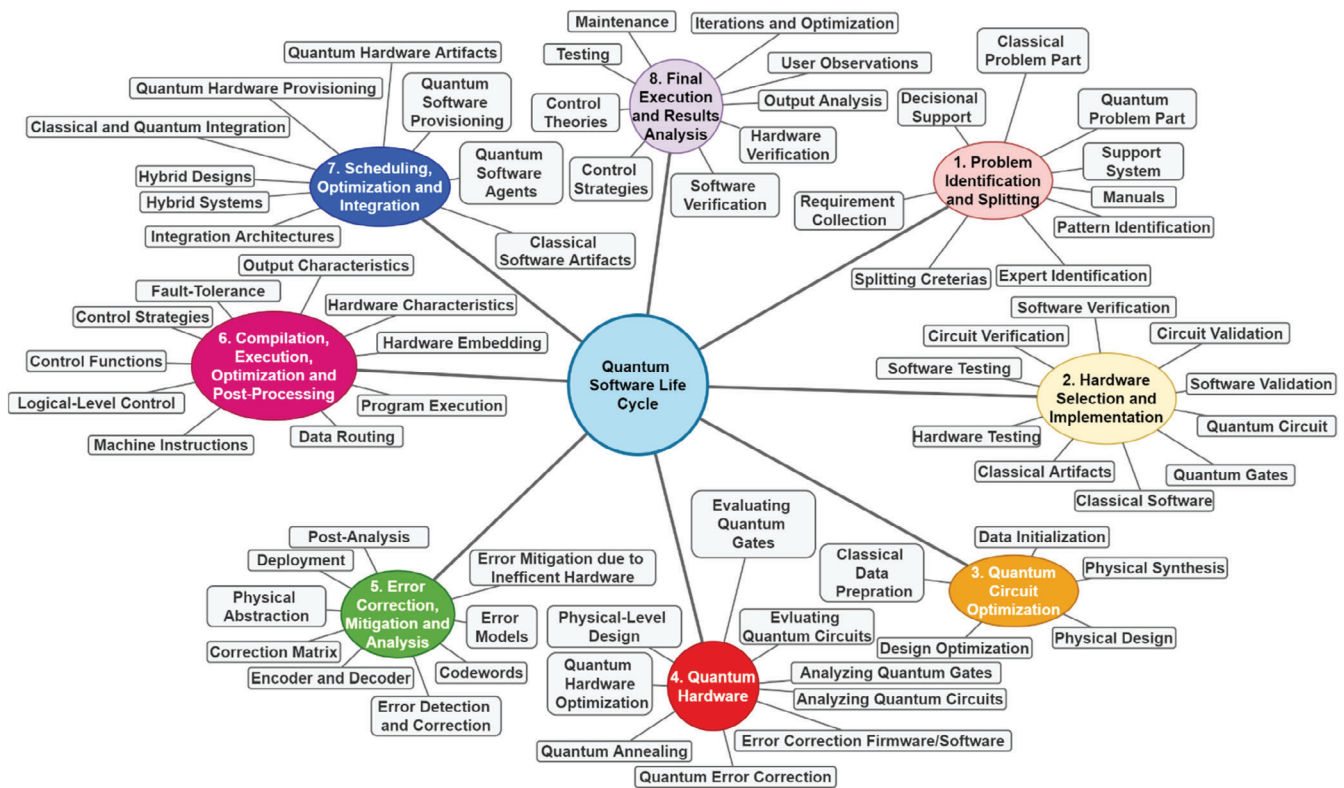


FIGURE 9 Quantum software life cycle and associated terminologies

5 | QUANTUM AND POST-QUANTUM CRYPTOGRAPHY

Quantum and post-quantum cryptosystems are the completely independent world. Quantum cryptography is applying quantum mechanics to perform cryptography tasks. Quantum cryptography encrypts data at the physical network layer by using quantum mechanics' physics. Whereas, post-quantum cryptography or quantum-resistant cryptography uses mathematical techniques. These techniques depend on hard arithmetic problems, which quantum computers cannot answer. Post-quantum cryptography usually refers to algorithms that have the capabilities to secure against attacks. For example, quantum computers running Shor's algorithm can break the security of most standard and difficult-to-solve mathematical cryptography problems.^{20–22} Likewise, factoring and discrete logarithms, which are widely used in classical cryptosystems, can be solved efficiently on quantum computers. Thus, QC or processing has brought fundamental challenges to the classical cryptosystem. The major applications of quantum cryptography include dense coding, teleportation, prime factorization, faster and secure database searching, secure secret sharing, secure processing, secure one-to-one communication, secure communications across public networks using a quantum smart card and security for cloud and e-commerce computing environments. Quantum computers try every possible solution at same time. Likewise, quantum computers, like brute force attacks, attempt all possible solutions to classical cryptography challenges simultaneously. Thus, regardless of key length, the future of Data Encryption Standard (DES) and Rivest–Shamir–Adleman (RSA) is bleak. Thus, it is important to address whether a quantum machine defend itself against a quantum machine attack or not? In case of unlimited quantum key length, quantum cryptography is considered to be secure. One-time pad is an example of unlimited key length crypto-system. QKD is based on one-time pad. Thus, it is assumed to be secure. There are various ways to ensure secure QKD. For example, quantum drones (QD) and quantum satellites (QS) are recently explored to share keys and establish multimedia communications.^{149–153} Additionally, there are many challenges that are yet to address.¹⁵⁴ For example, (i) quantum nodes are indistinguishable entity in quantum networks. Quantum nodes can be a quantum a repeater, access node, or central control node. The major challenge in quantum node is the need to create an efficient buffer mechanism for storing key and meet the dynamic need of quantum network, (ii) to establish an efficient quantum link between nodes with higher key generation rate and lesser cost, (iii) to design and implement a hybrid network consisting of trusted nodes and active optical switches for

direct peer-to-peer channel establishment between any two quantum nodes, (iv) to explore the feasibilities of point-to-multipoint or single receiver and multiple distribution mechanisms in quantum information processing, (v) to make efficient and trusted quantum multi-path strategies for quantum information processing and distribution, and (vi) to make secure interface between classical system and quantum node for integrating the quantum networks with classical systems.

Post-quantum cryptosystem considers the presence of quantum adversary's challenges due to unique QC features such as no-cloning.²² Quantum cryptography is defined as quantum mechanical properties for cryptography tasks such as QKD, encryption/decryption, signature, authentication, and hashing.^{20–22,155} The major advantages of quantum cryptography include the usage of fundamental laws of physics rather than mathematics-based algorithms which are simple to use but counterintuitive and consume fewer resources. Post-quantum cryptography can be used in various government applications to ensure secure identity proofs. For example, identity-based applications and documents (epassport, national identity cards, and other travel documents) can be made secure with digital signature and encryption processes from quantum-attacks. Post-quantum cryptography can be used in information and communication technologies including networks, networking equipments, servers and network services (e.g., cloud services). Thus, it is an efficient tool for securing futuristic networks. Bringing post-quantum cryptography in automation world can lead to security in various futuristic applications like robotics in healthcare, autonomous vehicles (ground, aerial, and underwater), agriculture, and aviation. The major challenges that post-quantum cryptography need to address in future include

TABLE 5 Quantum cryptography approaches

Author	Year	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
Deutsch et al. ¹⁵⁶	1996	✓	×	×	×	×	×	✓	×	×	×	×	×	×	×	×	×	×	✓	×
Naik et al. ¹⁵⁷	2000	✓	×	✓	×	×	✓	×	×	×	×	×	✓	×	×	×	×	×	✓	×
Elboukhari et al. ¹⁵⁸	2010	✓	×	×	×	×	✓	×	✓	×	×	×	×	×	×	×	×	×	×	×
Bugge et al. ¹⁵⁹	2014	✓	✓	×	×	×	✓	✓	×	×	×	×	×	×	×	×	✓	×	✓	×
Jain et al. ¹⁶⁰	2014	✓	✓	×	×	×	✓	✓	×	×	×	×	×	×	×	×	×	×	✓	×
Bruss et al. ¹⁹	2017	✓	×	×	✓	✓	✓	✓	×	✓	×	×	×	×	×	×	×	✓	✓	×
Li et al. ¹⁶¹	2018	×	×	×	✓	✓	✓	✓	✓	×	×	×	×	×	×	×	×	✓	✓	×
Bennett and Brassard ¹⁶²	2020	✓	×	×	×	×	✓	×	×	×	×	×	×	×	×	×	×	×	×	×
Bhusal et al. ¹⁶³	2020	✓	×	✓	×	✓	×	×	✓	×	×	×	×	×	×	×	×	✓	✓	✓
Brassard et al. ¹⁶⁴	2000	✓	×	×	×	×	✓	✓	✓	×	×	×	×	×	×	×	×	×	✓	×
Durak and Jam ¹⁶⁵	2020	✓	✓	×	✓	×	✓	✓	×	×	×	×	×	✓	×	×	×	×	×	✓
Gras et al. ¹⁶⁶	2020	✓	✓	×	×	×	✓	×	×	×	×	×	×	×	✓	✓	×	×	×	×
Guo et al. ¹⁶⁷	2020	✓	×	✓	×	×	✓	✓	×	×	×	×	×	×	×	×	✓	✓	✓	×
Huang et al. ¹⁶⁸	2020	✓	✓	×	×	×	✓	✓	×	×	×	×	×	×	×	×	×	×	✓	×
Melhem et al. ¹⁶⁹		×	×	×	×	✓	✓	✓	×	×	×	×	×	×	×	×	×	×	×	×
Qi et al. ¹⁷⁰	2020	✓	✓	×	✓	✓	✓	×	×	×	×	✓	✓	✓	×	✓	×	✓	✓	×
Shang et al. ¹⁷¹	2020	✓	×	×	✓	×	✓	✓	×	×	×	×	×	×	×	×	×	×	✓	×
Trushechkin ¹⁷²	2020	✓	×	×	×	×	✓	×	×	×	×	×	×	✓	×	×	×	×	×	×
Vybornyi et al. ¹⁷³	2020	✓	×	×	×	✓	✓	✓	×	×	×	×	×	×	×	×	×	×	✓	×
Yin et al. ¹⁷⁴	2020	×	✓	×	✓	✓	✓	✓	×	×	×	✓	×	✓	✓	✓	✓	✓	✓	×
Zhang et al. ¹⁷⁵	2020	✓	×	✓	×	×	✓	✓	×	×	×	×	×	✓	×	×	×	×	×	✓
Zhou et al. ¹⁷⁶	2020	✓	✓	×	×	×	✓	×	×	×	×	×	✓	×	×	×	×	×	×	✓

Note: A. Communication protocols, B. Implementation, C. Simulation, D. Quantum authentication, E. Quantum encryption, F. Quantum key distribution, G. Quantum attack detection and analysis, H. Short survey associated with implementation, I. Long survey for in-depth analysis, J. Quantum programming, K. Long-distance entanglement, L. Short-distance entanglement, M. Efficiency-mismatch attack, N. Detector-blinding attack, O. Detector dead-time attack, P. Beam-splitter attack, Q. Spatial-mode attack, R. Eavesdropping attack, S. Data analysis/machine learning.

(i) limit the size of encryption keys or keys used in signature without compromising over security, (ii) the encryption or decryption mechanisms are required to be time efficient for each quantum network entity including quantum communication channel or quantum node, (iii) to reduce the amount of traffic in encryption/decryption or signature processes, (iv) to make an era of QC, quantum algorithm, quantum tool and techniques, quantum technologies, and mathematical standards for speed-up the security scenarios, (v) to provide high bandwidth possibilities for existing network infrastructure and architecture for handling the high traffic scenarios due to post-quantum approaches, and (vi) copying quantum state's encoded data is not feasible, and this reduces the chances of attack and increases the probability of eavesdropping detection, better performance as compared to traditional cryptography, and so forth. Thus, designing efficient buffer-based quantum network device need to be taken in future. Table 5 shows a comparative analysis of quantum cryptography approaches designed and experimented with during recent times. These approaches are classified based on various parameters including designed or experimented for communication protocols, implementation, simulation, quantum-based authentication mechanisms, quantum-based encryption/decryption operations, QKD, quantum attack detection and analysis, short survey, long survey, approaches using programming for quantum operations, long or short-distance entanglement, attacks (efficiency-mismatch, detector-blinding, detector dead-time, beam-splitter, spatial-mode, eavesdropping), and approaches where data analysis is performed either using machine learning.

Figure 10 shows the classification of quantum cryptography challenges. The challenges are categorized into four major categories, including security attacks and challenges, hardware challenges, performance and cost-related challenges, and quantum-related design challenges. The majority of security attacks and challenges considered various types of security attacks and their feasibility in the quantum world; hardware challenges include experimentation issues whose performance is affected by the hardware used. Performance and cost-related challenges include reducing the cost while improving the performance parameters. Finally, design challenges include developing novel quantum protocols, tools, or techniques while addressing the challenges of existing real-time experimentations.

5.1 | Quantum key distribution

QKD is an effective way of protecting information security using quantum computers.^{56,177} As compared to traditional cryptography-based key distribution mechanisms, which are vulnerable to computational power-based scenarios,

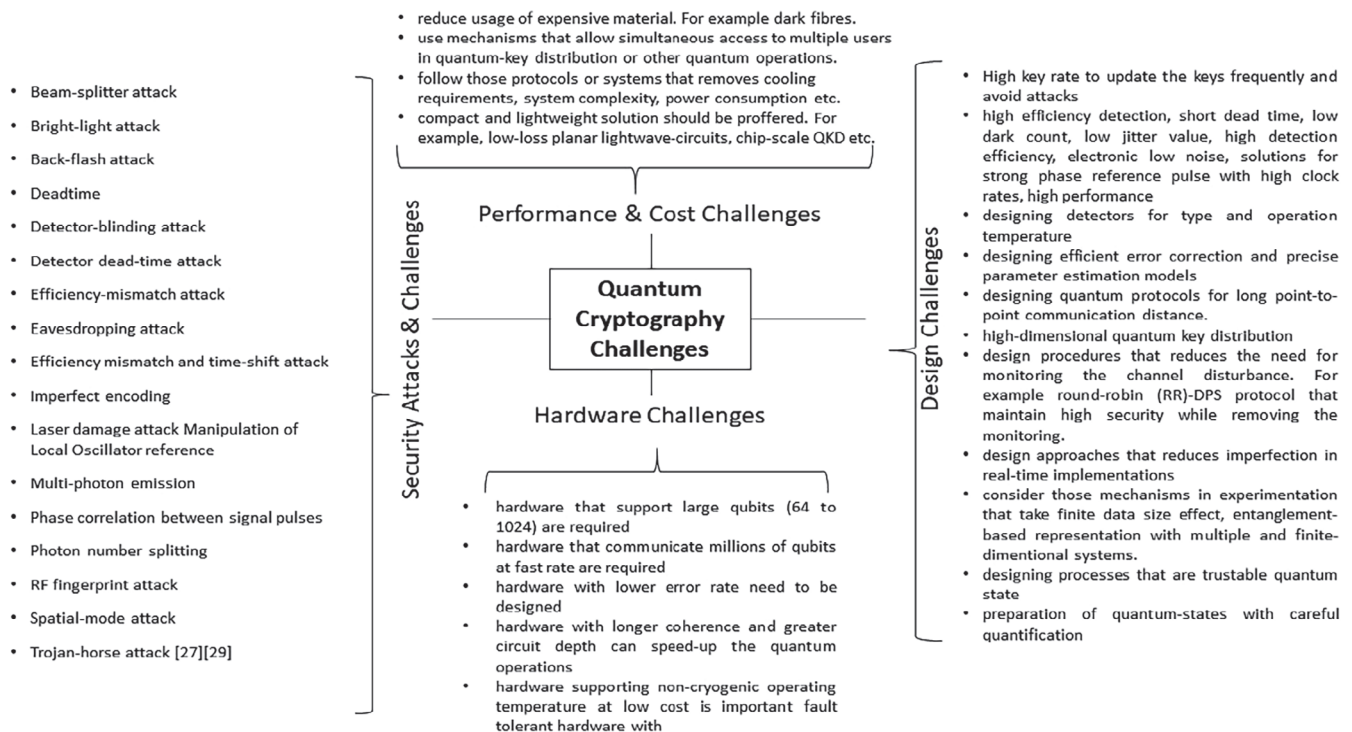


FIGURE 10 Quantum cryptography challenges

a quantum cryptography mechanism (like QKD) is secure against various attacks. In quantum cryptography, the no-cloning theorem¹⁷⁸ in quantum mechanics states that it is impossible to make a perfect copy of the quantum system or its states. Thus, any eavesdropping attempt adds noise to the quantum transmission that is easily detectable by two parties (source and destination).¹⁷⁹ QKD protocols can be classified based on the use of properties during transmission including applied modulation, encoding/decoding, and quantum channel implementation. Likewise, there are various types of QKD approaches.^{180,181} Table 6 shows the comparative analysis of these approaches, which are discussed below.

TABLE 6 Comparative analysis of QKD

Type of CV-QKD	Pros	Cons
Gaussian-modulated CV-QKD	<ul style="list-style-type: none"> Security analysis is much more advanced compared to discrete-modulated CV-QKD. 	<ul style="list-style-type: none"> Distance limitation for secure QKD is a major concern. The use of high-performance error-correcting code can improve security but reduces the distance coverage.¹⁸²
Discrete-modulated CV-QKD	<ul style="list-style-type: none"> More suitable for long-distance secure key transmission. Simple experimentation setup. Great potential for large-scale deployment in secure quantum networks. The integration of post-selection strategies with reverse reconciliation can significantly improve the key rates. 	<ul style="list-style-type: none"> Security analysis in this system is more challenging compared to Gaussian-modulated CV QKD because analysis relies on the linearity of the channels which is not an easy condition for verification.
Coherent on-way (COW) quantum key distribution	<ul style="list-style-type: none"> Simple in experimentation. Reduce interference visibility. Avoid photon number splitting attack to a large extent. Falls in distributed-phase-reference QKD category. 	<ul style="list-style-type: none"> Empty pulses contain a light that can introduce noise. This can increase error rates. Performance decreases with an increase in disturbances. Small disturbances do not affect performance.
Differential phase-shift (DPS) quantum key distribution	<ul style="list-style-type: none"> Falls in distributed-phase-reference QKD category. Integration with randomness or improved transmitter can reduce the disturbances and improve the performance.^{183,184} 	<ul style="list-style-type: none"> Chances of side-channel attacks are higher. Thus, techniques (e.g., attenuation) are required to be integrated for removing it. Performance decreases with an increase in disturbances. Small disturbances do not affect performance.
Six-state quantum key distribution	<ul style="list-style-type: none"> Using this category of protocols, a high error-rate can be detected easily in the presence of any eavesdropping attack. The speed of communication lies in the high-speed key distribution category. The probability of interference, collective attack, and obtaining the secret is low. 	<ul style="list-style-type: none"> Chances of obtaining the secret cannot be completely avoided. Need to analyze the hidden variable models for protecting the protocols against attacks. Multiple eavesdropping challenges to top-level authenticated communication need to be addressed.
Decoy-state quantum key distribution	<ul style="list-style-type: none"> A high secure key rate can be generated using the decoy-state protocol. The problem of lower secure key rate can be efficiently handled with inequality based statistical models. Found to be an effective method in avoiding the photon-number splitting attack. 	<ul style="list-style-type: none"> The secure key rate can be lower down to a significant level if parties' parameters are varied with different decoy states. Usage of different decoy states is not yet experimented in realistic scenarios to confirm its adaptability with security. Computational power challenge also reduces the secure key rate and can cause statistical fluctuations.

5.1.1 | Discrete and continuous variable QKD

QKD can be designed in both discrete and continuous variables. Some of these approaches are briefly discussed as follows. Ghalaii et al.¹⁷⁸ discussed the Gaussian and non-Gaussian modulated continuous-variable QKD (CV-QKD) methods. Further, the non-Gaussian CV-QKD protocol is extended with a discrete modulation approach for increasing the secret key rates. Besides, the proposed mechanism is found to support the discrete-modulation CV-QKD over CV quantum repeaters and to long-range system operation in-live. Valivarthi et al.¹⁸⁵ proposed a plug-and-play CV-QKD with Gaussian modulation quadratures. In experimentation, two independent fiber stands have been used for two narrow line-width lasers for quantum signal transmission. This experimentation increases the secret key rate up to 0.88 Mb/s with different experimental setups and inputs. This experimentation is considered to be an effective mechanism in terms of low-cost deployment for metropolitan optical networks. The investigation is useful in terms of its design, use of Raleigh back-scattering mechanism to minimize noise, and integration of GG02 symmetric protocol with heterodyne detection.¹⁷⁹ The complete setup makes the proposed QKD faster and secure. Leverrier and Grangier¹⁸⁶ presented a CV-QKD protocol combining discrete modulation and reverses reconciliation. The protocol is tested experimentally, and it is observed that the proposed scheme can distribute the secret key over a long distance while ensuring security. Li et al.¹⁸² proposed a discrete modulated CV-QKD scheme that improves the system performance and secure distance with machine-learning-based detectors. The proposed scheme is capable of processing the secret keys to improve the overall system performance. Lin et al.¹⁸⁷ applied numerical methods to analyze the security aspects in discrete modulated CV-QKD. The two proposed variants of discrete-modulated CV-QKD are capable of generating much high key rates for longer distances as compared to binary or ternary modulation schemes. Thus, aim of this approach is to generate high key rates for longer distances as well. Ruan et al.¹⁸⁸ analyzed optical absorption and scattering properties of discrete-modulated CV-QKD. It is observed that the performance of four and eight-state protocol in asymptotic and finite-size cases is dependent on seawater composition, that is, if the composition is complex, then the performance of protocol decreases as well. The variation in optical modulation and minimizing the extra noise can improve the protocol's performance. In another observation, it was found that the number of states improves performance. In this case, the performance of the eight-state protocol is better compared to the four-state protocol. In recommendations, CV-QKD is found to be significant over the seawater channel and provides a good medium to construct a secure communication network.

5.1.2 | Coherent on-way quantum key distribution

In COW QKD, logical bits are encoded and emitted with a sequence of weak coherent pulses. These pulses may be tailored from a laser having an intensity modulator. Various mechanisms are used to make COW QKD practical. Some of the recently discussed approaches are explained as follows. Stucki et al.¹⁸⁹ presented a COW-QKD protocol with weak coherent pulses. The simplicity of this experimentation increases the bit rates and reduces interference visibility as well. This protocol achieves a high efficiency for secret bits per qubit generation while lowering the photon number splitting attacks. Maufu et al.^{190,191} realized the importance of the differential-phase-reference category of QKD protocols. In this category, there are mainly two types of QKD protocols, including COW and differential phase shift. Maufu et al.¹⁹¹ formalized the COW-QKD protocol with non-computing positive operator-value measures (POVM). This formalization increases the chances to have unconditional security proof against general attacks. The POVM elements, effective for generating security proofs against attack, include measurement probabilities and positive operators, composite measures, all types of measurements distinguishing between two quantum states, and an informationally complete secure state. Maufu et al.¹⁹² reanalyzed the necessary condition requirements with non-commuting POVM elements-based COW protocol. The major challenge considered in stating unconditional security proof is the class of protocol that uses coherent signals. These coherent signals are not symmetric as compared to qubits used in proof realization. Thus, there is a need to formalize the COW QKD protocol without disclosing the detailed working explanations and parties' confidentiality. It is observed that POVA elements can make this possible with high-security standards. Wonfor et al.¹⁹³ conducted a trial of the COW-QKD protocol with a commercial-grade encrypted system. In experimentation, a link is launched for QKD with 500 Gbps encrypted data transmitted over a distance of 121 km. As result, it is observed that QKD in O-band COW protocol with free detectors and C-band DWDM channels gives a stable performance for many weeks. Further, 25 DWDM channels with co-propagation can make the QKD process feasible while ensuring security proofs.

5.1.3 | Differential phase-shift quantum key distribution

In DPS QKD, a highly attenuated coherent pulse with phase shift is sent from the sender side and is received with a one-bit delay at the receiver side. It is a long since this approach was developed. However, several variations of this approach are studied in recent times. Some of these approaches are discussed as follows. Alhussein and Inoue¹⁹⁴ realized the importance of side-channel attacks in the DPS-QKD system. DPS-QKD protocol is found to be another simple and efficient protocol because it works in cases when precise synchronization of signals between distant parties is not possible. The proposed scheme has avoided the control of blinding and controlling side-channel attacks. To detect a side-channel attack at Bob's side, a variable attenuator is added at random and occasional attenuation inserted. Further, the performance is analyzed, confirming the adaptability of the proposed approach. Collins et al.¹⁹⁵ experimented with the quantum digital signatures transmission over a long distance (90 km) using the DPS-QKD protocol. The authors claimed that the transmission was aimed to be conducted for long-distance compared to previous works. The distribution of quantum digital signatures ensures message integrity as well as non-repudiation. Further, the performance of the proposed scheme is comparable to the BB84 protocol used for QKD with 1550 nm wavelength and similar experiment settings, including clock rate and transmission distance considered for the operation. Hatakeyama et al.¹⁸³ experimented with a round-robin DPS-QKD protocol to reduce the bit error rates. The experiment is conducted to take advantage of simple DPS-QKD functioning to increase tolerance without compromising on security issues. This work has extended with basic DPS-QKD protocol with randomness. The randomness and few additional delays increase the performance of the proposed protocol as compared to the basic DPS-QKD protocol. The simulated experimentation and key generation rates are analyzed with different randomness patterns. It is observed that the performance of the proposed protocol can be significantly increased with a few parameter changes. Schrenk et al.¹⁸⁴ developed a low-complexity transmitter for DPS-QKD. This transmitter uses an integrated laser device with two electro-optic elements. This experimentation observed the quantum state preparation and chances of side-channel attacks with the proposed transmitter mechanism. A distributed environment with a centralized quantum receiver shows the performance of form-factor and successful deployment at a short-term distance. Overall, the performance of the whole system is found to be effective for QKD compared to generalize DPS-QKD. Sibson et al.¹⁹⁶ identified a low error rate; high speed clocked QKD operation of indium phosphide transmitter chip useful in the telecommunications industry. This configuration has experimented with three protocols, including BB84, coherent one way, and different phase shifts. Results show that the proposed approach gives better performance without impacting the security standards, and they are useful for any sort of communications in telecommunication networks.

5.1.4 | Six-state quantum key distribution

In six-state quantum cryptography protocols, BB84 protocol is extended to use six-state polarization ($|0\rangle$, $|1\rangle$, $|+i\rangle$, $|-i\rangle$, $|+\rangle$, $|-\rangle$) on three orthogonal bases. Further, the six-state protocol can tolerate a noisier channel and detect higher rate errors during any eavesdropping attack. The six-state protocol can be implemented either using a quantum computer or optical technologies. For example, Lo¹⁹⁷ derived the proofs for unconditional security solutions in six-state QKD protocols. In this implementation, it has been observed that unconditional security could lie at a high bit error rate of 12.7% as compared to 11% in the BB84 protocol. The proposed technique has used DiVincenzo, Shor, and Smolin's quantum codes for bit-flip and phase error pattern analysis. It has been observed that bit-flip error syndromes entropy can be used for a phase error pattern that increases the security of the proposed protocol at a high error rate as well. Similarly, Azuma and Ban¹⁹⁸ realized the security of the six-state QKD protocol against various attacks, including intercept/resend, collective, and eavesdropping. Here, the probability of an attacker's interference in legitimate user communication is noticed, and the chance of obtaining the secret is measured. In collective attack observations, the security level is found to be high that can protect imposing looser constraints upon the attacker's strategies. This work has considered the comparative analysis of proposed security-level detection with the E91 protocol. Results show that the six-state protocol is comparatively secure against attacks if hidden variable theories are examined with a small disturbance of $1/3$. Chau et al.¹⁹⁹ identified that four-dimensional qubits in QKD are possible, and it can have security equivalent to the six-state scheme with arbitrarily long raw key size. Here, the tolerance level is observed to be 21.6% using one-way classical communication with passive basis selection in decoy. Thus, an increase in security level with a high key rate meets the requirements of the current QKD.

5.1.5 | Decoy-state QKD

The decoy-state QKD protocol is preferred over others because it provides better conditional or unconditional constraints over the gain and the error rate of single-photon states. In recent times, various amendments are made to improve the decoy-state QKD protocol. For example, Liu et al.²⁰⁰ realized the importance of decoy-state QKD protocol and its capability to protect against photon-number splitting attacks. In this work, two-basis detector efficiency asymmetry was found to be existing in real experimentation. To improve the rate of QKD with asymmetric basis-detector efficiency asymmetry, this work has investigated a 4-intensity decoy-state optimization protocol to protect against attacks. In observation, it is found that X and Z basis efficiencies are not the same, and the practicality of decoy-state has high chances. Grasselli and Curty²⁰¹ focused on twin-field (TF)-QKD protocol because of a secure secret-key mechanism. It has been observed in an analysis that the security of this protocol is associated with photon-number states using the decoy-state method. This work has derived analytical bounds on the parameters used by parties and concluded that either two, three, or four decoy intensity settings could be used for investigating the protocol's performance. In further observations, the protocol is found to be robust against optical pulses' fluctuations. Chau and Ng²⁰² made various observations in the decoy-state protocol. In the first observation, it is found that a secure key rate can be seriously lowered down with the deviation of single-photon. In their second observation, the error rate can also lower the secure key rate by bounding the yields and usage of the type of decoy. To improve the secure key rate in such conditions, McDiarmid inequality is found to be effective because it helps in computing the lower bound in the centering sequence method. As result, it has been observed that the secure key rate can be doubled with the proposed approach for a realistic 100 km long quantum channel. This work has introduced a powerful inequality technique for handling problems beyond statistical data with the central limit theorem. Liu et al.²⁰³ applied the chernof bound to passive decoy-state and improved the final key rate. In experimentation, it is claimed that the proposed approach can securely transmit the data over 205 km, which is close to an asymptotic limit of 212 km. This is found to be the highest key rate over a long distance compared to existing approaches. In conclusion, the majority of decoy-state protocols are used either to improve the secure key rate or its transmission over a long distance.

5.2 | Post-quantum cryptography

The post-quantum cryptosystem is defined as the set of cryptography primitives and protocols that are secure against quantum computer attacks.^{54,55,204–206} It is observed that the existing cryptography primitives and protocols rely on mathematical problems such as integer factorization, discrete logarithm, and elliptic-curve discrete logarithm.⁵⁸ With the possibilities of quantum computers, it is theoretically proved that all of these mathematical problems could be solved in a short duration.¹⁹² Thus, post-quantum cryptography is widely discussed. The protocols in post-quantum cryptography are mainly classified into five categories: code-based, lattice-based, supersingular elliptic curve isogeny, multivariate, and hybrid, as shown in Figure 11.

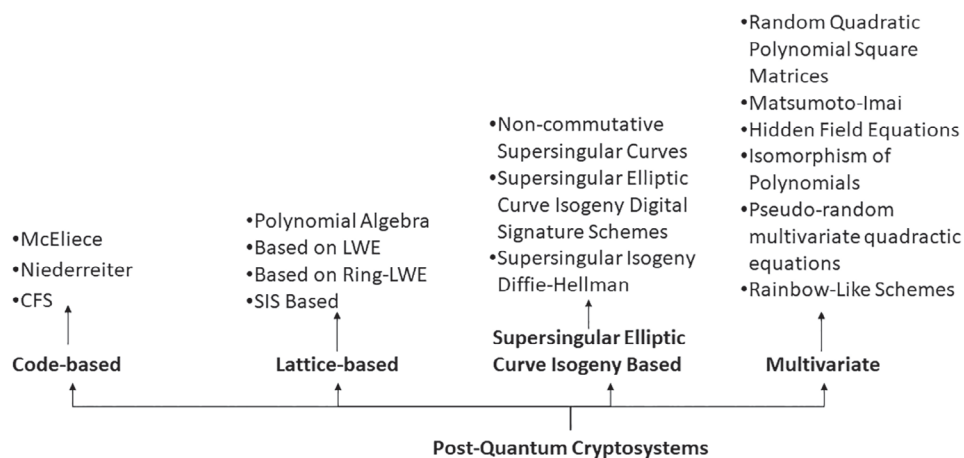


FIGURE 11 Post-quantum cryptography protocols

5.2.1 | Lattice-based cryptosystem

In mathematics, lattice is an arrangement of regularly spaced points in a subgroup R^n that is isomorphic to another group Z^n such that R^n is isomorphic to Z^n , that is, all combinations of vectors in space lies in R^n . Ajtai²⁰⁷ initiated the use of cryptography in the lattice-based system and derived the computationally hard problems on lattices. The computational hard problem provides security and is found to be useful in other cryptography primitives such as homomorphic cryptography, attribute-based cryptography, and code-based cryptosystem. In References 208–211, a lattice class of small integer solution (SIS) and its inhomogeneous variants are discussed. For example, Ring-SIS²⁰⁸ is a variant of the lattice-based cryptosystem. This variant is having an issue of difficult to solve for any randomly selected instance. This property makes this variant a class of average-case problems and it is not sufficient to have worst-case complexity applications supporting SIS or Ring-SIS variant. Like other lattice-based cryptosystems, SIS and Ring-SIS variant also falls in the NP-hard problem. As compared to a lattice-based system with worst-case hardness, SIS and Ring-SIS are likely to secure against quantum computers. In recent studies, lattice-based schemes are more focused on shifting from worst-case to average-case security perspectives. Thus, breaking the randomly chosen instance in lattice-security schemes and finding a solution for worst-case instances of the lattice-based system are important concerns.

Langlois and Stehlé²¹² compared the average-case reduction problems with module lattices in a lattice-based system. The security of both systems is found to be comparable. Cryptosystems based on worst-case to average-case reduction analysis were found to be more secure because of converse reductions. Schemes based on ideal lattices, having structured objects, provide higher security. Assessing those schemes which use ideal lattices to ensure high security need to be assessed to standardize the lattice problems for more general and specific classes of lattices. Exploiting the ideal lattices or module lattices with a certain degree of module rank would impact the lattice-based cryptosystem. The hardness of various schemes (like Ring-SIS, R-LWE) would be impacted with successful ideal lattice exploitation. Plantard and Schneider²¹³ compared the ideal and general lattices and started the experimentation to create challenges for ideal lattices. It is assumed that the security challenges of lattice-based cryptosystems lie in ideal lattices. Thus, security assessments of ideal lattices are studies in recent work for both SIS and LWE-based lattice cryptosystems. Lyubashevsky et al.²¹⁴ explored the ideal lattices in ring signature and confidential transactions. With the use of ideal lattices, the issue of small output, storage and processing can be achieved. Reducing the transaction size and other requirements make lattice-based cryptosystem a viable candidate for resource-constraint networks like IoT networks. The transaction size is an important parameter to consider for employing lattice-based schemes in networks. So far, it is assumed that transaction size depends upon security parameters but efforts are done to reverse this assumption and make it possible for more applications. Various lattice-based cryptosystem approaches are summarized in Table 7 with comparative analysis of their primitives in Table 8.

TABLE 7 Lattice-based cryptosystem approaches

Lattice-problem	Variants	Pros	Cons
SIS and its inhomogeneous variants	Ring-SIS, ²⁰⁸ Bi-GISIS, ²⁰⁹ Lattice-based Direct Anonymous Attestation (LDAA), ²¹⁰ Certificateless Signature (CLS) scheme on NTRU lattice. ²¹¹	Smaller storage and faster operations are preferred. Schemes, like LDAA, are secure against weak/strong deniability attacks.	Weak/strong deniability is the least addressed. The SIS problem becomes solvable in polynomial time with various parameter variations.
Learning with errors (LWE)	Ring-LWE, ^{208,209} MPSign, ²¹⁵ Decision-LWE, ²¹⁰ Decision-Ring-LWE, ²¹⁰ LDAA, ²¹⁰ Module-LWE, ²¹⁶ Module-Learning With Rounding (M-LWR), ²¹⁷ NewHope, ²¹⁸ Kyber, ²¹⁸ R. EMBLEM, ²¹⁸ KCL, ²¹⁸ OKCN/AKCN-RLWE, ²¹⁸ AKCN-MLWE, ²¹⁸ ILWE, ²² MPLWE. ²²	Smaller storage and faster operations are preferred. Polynomial-based LWE allows for secrets that are much smaller compared to modulus operations. In results, schemes are faster.	There are equally likely chances of chi-square attack, cyclotomic vulnerabilities, inherent structure exploitability, and sensitive dependence to field parameters in the majority of existing schemes. Weak/strong deniability is the least addressed.

TABLE 8 Comparative analysis of lattice-based cryptography primitives

Author	Major observations	Year	A	B	C	D	E	F	G	H
Banerjee et al. ²¹⁶	A Low-power crypto-processor is designed, configured, and tested to accelerate polynomial arithmetic operations. Lightweight cryptography primitives and protocols are combined with sampling techniques. This accelerates the polynomial sampling in discrete distribution parameters useful in lattice-based schemes.	2019	✓	✓	✓	✓	✓	✓	✓	✓
Nejatollahi et al. ²²	Surveyed lattice-based cryptographic schemes, security challenges in software and hardware implementations, and technology adoption	2019	✓	✓	✓	✓	×	✓	✓	✓
Akleyek and Seyhan ²⁰⁹	An authentication key exchange-based scheme is designed using the Bi-GISIS problem. Comparative analysis with SIS and LWE problems is performed. Testing of the proposed approach with a security model is conducted.	2020	✓	✓	✓	✓	×	×	✓	✓
Bai et al. ²¹⁵	A polynomial LWE-based digital signature scheme is proposed and found to be secure with a quantum-access random oracle model. This work has observed an efficient key-recovery attack against homogeneous polynomial SIS problems with small secrets.	2020	✓	×	✓	✓	×	×	✓	✓
El Kassem ²¹⁰	In this work, smart zero-knowledge proofs are designed and explained for lattice problems.	2020	✓	✓	✓	×	×	×	✓	✓
Mera et al. ²¹⁷	Designed and experimented with a polynomial multiplier using the Toom–Cook algorithm for cryptoprocessors in the lattice system. Usage of the proposed hardware-based system is tested for cryptography primitives especially public key protocol.	2020	✓	×	×	✓	✓	×	✓	✓
Nejatollahi et al. ²¹⁸	This work has explored the design space of a flexible and energy-efficient post-quantum cache-based hardware accelerator for five different submissions.	2020	✓	✓	✓	✓	✓	✓	✓	✓
Xu et al. ²¹¹	Proposed quantum attack resilience certificateless signature scheme with the difficulty of small integer solution on the NTRU lattice.	2020	✓	×	✓	✓	×	×	✓	✓

Note: A. Encryption/decryption, B. Authentication, C. Digital signature, D. Key distribution, E. Cryptoprocessor design, F. Identification scheme, G. Lattice-based approach for application, H. Protocol design/development/implementation/simulation.

5.2.2 | Code-based cryptosystem

Robert McEliece initiated the code-based cryptography based on NP-hardness of the syndrome decoding problem (SDP).²¹⁹ A code-based cryptosystem relies on secretly decoding the linear code having a predefined structure. McEliece scheme is based on binary Goppa codes (as linear code) with the Nicholas Patterson algorithm in the decoding process. McEliece cryptosystem is fast in its encryption and decryption operations. The major drawback of the McEliece cryptosystem is the use of large key sizes that make this scheme infeasible for resource-constrained devices. In literature 220–224, various variants of the McEliece scheme are proposed using different error-correcting codes such as rank ECC, Gabidulin codes, twisted Gabidulin codes, twisted Reed–Solomon codes, low-density parity-check (LDPC) codes, quasi-cycle codes, and quasi-cyclic low-rank parity-check (QC-LRPC). Among other code-based cryptosystems,²²⁴ Niederreiter and CFS (Courtois, Finiasz, Sendrier) cryptosystems are also very popular. The CFS system is found to be useful for Internet of Things (IoT) signature schemes with Fiat–Shamir transformation.²²⁵ Both Niederreiter and CFS schemes generate small

TABLE 9 Analysis of contributions in code-based cryptosystems

Author	Cryptosystem	Error-correcting codes (ECC)	Major strengths
Jäämeri ²²⁰	McEliece, Gabidulin-Paramonov-Tretjakov (GPT)	Rank ECC, Gabidulin codes, Twisted Gabidulin codes, Twisted Reed-Solomon codes	Protected from structural weaknesses and Overbeck's attack
Singh ²²¹	McEliece, Niederreiter, Classic McEliece	Linear codes, Goppa codes	Strongly protected against brute force attacks. Lesser disclosure of secret information can protect the schemes from total break, global deduction, local deduction, information deduction, and distinguishing algorithms.
Bardet et al. ²²²	McEliece	Gabidulin codes, Reed-Solomon codes, Linear codes	Identified an attack that is below the security level for all rank-based schemes available in NIST post-quantum processes. The proposed attack is useful for systems having small to medium scale parameters that require lesser memory compared to the best quantum attacks.
Ezerman et al. ²²³	McEliece, Niederreiter	Goppa codes	A secure signature scheme is designed using a code-based cryptosystem. It is observed that the signature schemes in a code-based cryptosystem can be classified as "hash-and-sign" or "Fiat-Shamir." The proposed scheme is a group signature scheme that requires multi-layered operations for generating group signatures.
Fernández-Caramés ²²⁴	McEliece, Niederreiter	Goppa codes, Low-Density Parity-Check (LDPC), Moderate-DPC (MDPC), Quasi Cycle Codes (QCC), Quasi-Cyclic Low-Rank Parity-Check (QC-LRPC), LRPC, LDPC	Conducted an in-depth survey of various post-quantum cryptosystem approaches and their variants. The survey is focused on protecting the IoT systems using post-quantum computing. Further, IoT architectures and challenges are analyzed for providing guidelines to secure future post-quantum IoT systems.

signatures that result in fast computations. Table 9 shows the analysis of a few recent contributions in code-based cryptosystems. Various code-based cryptosystem approaches can be classified based on two sets of problems: SDP and the hardness of distinguishing a code from pseudorandom code. These problems and their interconnection with code-based cryptography are explained as follows.

- *Syndrome decoding problem:* This is the first set of problems for several code-based algorithms. Over the development of a code-based cryptosystem, the complexity of the syndrome problem is increasing. However, SDP-based code-based cryptosystems share design and complexities. Their complexities rely on Grover or quantum walks. Cayrel et al.²²⁶ discussed the computational efficiencies of linear programming to perform real-time message recovery attacks. This is a message-recovery laser fault injection attack over a code-based cryptosystem. This attack experiments over the classic McEliece cryptosystem in a worst-case scenario. There are many adversaries or attack feasibilities studied during the recent time in the worst-case scenario. However, an average-case scenario in any post-quantum cryptosystem is considered to be much secure. A reference to this attack to the Niederreiter cryptosystem is also discussed. A large set of code-based cryptosystems and studies are based on either McEliece or Niederreiter cryptosystems.^{220–224} The chances of attack increase with more faults in syndrome decoding or fault injection reduction in computational complexity scenarios (like in IoT). With an increase in vulnerabilities, the chances of other attacks like secret error-vector disclosure with efficient linear programming or strong parameter disclo-

sure in cryptosystems. It has been observed that the chances of any form of these attacks increase with variations in the fraction of faulty syndrome entries. Ezerman et al.²²³ discussed the hardness of McEliece and the syndrome decoding problem for group signature schemes using code-based cryptography. This scheme applies anonymous and randomness to ensure group signature. Authors have focused on implementing this approach and suggested improving the performance in implementation, applying standard model or quantum random oracle model to get better experiences.

- *The hardness of distinguishing a code from pseudorandom code:* Rank metrics play important role in various applications associated with code-based cryptography. Few applications include space-time coding, network coding, and asymmetric key-based cryptosystems.^{227–229} Hardness is a theoretical property of a code. In code-based cryptography, the hardness of a distinguishing code can help in removing the error which in turn avoids attacks. Couvreur et al.²²⁹ discussed the importance of indistinguishability under chosen-plaintext, chosen ciphertext, and adaptive chosen-ciphertext attacks in network coding-based post-quantum cryptography. Jäämeri²²⁰ discussed the importance of a code-based cryptosystem with those schemes that are protected from structural weaknesses and Overbeck attacks. However, indistinguishability is a major challenge. The required security levels with certain overhead and randomness in the encryption scheme can be achieved. Singh²²¹ discussed McEliece, Niederreiter, and Classic McEliece-based cryptosystems. The cryptosystems based on these schemes are well protected from various attacks with different coding schemes. However, the hardness of the rank metric is required to ensure security in various applications like post-quantum cryptography security with network coding.²²⁷ Bardet et al.²²² discussed the algebraic attack on the rank metric in a code-based cryptosystem. In this study, McEliece and Niederreiter cryptosystems are used. It has been observed that weakness in rank metrics can result in algebraic attacks. Thus, there is a need to consider the hardness of a code in a rank metric. In an alternative solution, complexity bound could be applied to ensure the hardness of rank metric which in turn ensures the security of a cryptosystem.

5.2.3 | Multivariate cryptosystem

In multivariate cryptosystem, NP-hard and NP-complete multivariate equations are considered. The efficiency of a multivariate cryptosystem is based on the difficulty level in solving the systems of quadratic equations over a field. The concept of “one-way functions” composes of multiple easily invertible maps that could result in a difficult to invert function without much knowledge of individual sub-function in composition. Multivariate cryptosystem has many mature systems compared to other post-quantum cryptosystems because it started much earlier. The major advantage of multivariate cryptosystem includes fast processing, less computational and communicational resource requirements,²³⁰ and small signature generation in lesser polynomial time. Multivariate cryptosystems are largely classified into a digital signature, encryption/decryption, and other public-key cryptosystem-based approaches. In Reference 231, NIST first round process is explained. There are a total of three rounds so far in post-quantum cryptography. In the third round, seven finalists and eight alternatives are selected for post-quantum cryptography. Cartor²³² discussed multivariate cryptography, the important direct algebraic attacks, differential techniques, and proposed a new multivariate encryption scheme. The proposed scheme is analyzed against algebraic, MinRank, discrete differential, and parameter selection-based attacks. The theoretical analysis gives a detailed picture of the multivariate scheme. However, practical aspects and their analysis are missing. Thus, this work can be extended to analyze the implementation aspects, performance analysis, and integration with application scenarios. Smith-Tone and Tone²³³ studied the random linear code scheme-based nonlinear multivariate cryptosystem. This work has integrated the code-based and multivariate-based post-quantum cryptosystems. Thus, maximum security advantages can be taken out of it. Although this work has tested the proposed approach against various attacks this work can be extended to consider testing against weaknesses of code-based cryptosystems like hardness in indistinguishability of a code in a rank metric. In Reference 234, the integration of a multivariate scheme with Blockchain is proposed. Here, an elliptic curve-based digital signature scheme and the Rainbow algorithm are used for creating a Blockchain. Security levels are varied from 80 bits to 256 bits and signature size, public and private key size variations are observed for two algorithms (Rainbow and Elliptic curve based digital signature scheme). This work has proposed the Ethereum network for analysis. However, this work can be extended to explore the private, public, and consortium-based Blockchain network for specific applications. Table 10 shows an analysis of multivariate cryptosystems.

TABLE 10 Analysis of multivariate cryptosystems

Cryptosystem	Variants	Major strengths
Multivariate digital-signature schemes ^{231–233,235}	Rainbow digital signature schemes, Tame Transformation Signature (TTS), Tractable Rational Map Signature (TRMS), GeMSS, LUOV, MQDSS, Oil and Vinegar, Unbalanced Oil and Vinegar, Rainbow, CyclicRainbow, RainbowLRS2, Circulant Rainbow, NC-Rainbow.	Multivariate digital-signature schemes are comparatively more secure than multivariate encryption/decryption or public-key cryptosystem because short signatures are difficult to solve in polynomial time. Simple arithmetic operations (addition and multiplication) make the schemes much efficient, especially for low-cost devices. Multivariate schemes are considered to have very high security with small signature length. For example, the GeMSS scheme is found to achieve the NIST PQCSP level V security standard in the first round.
Multivariate encryption/decryption schemes ^{232,233,235,236}	EFLASH, C* Toy, PFLASH, C*, SFLASH, Hidden Field Equation (HFE), HFE ⁺ , ABC, SRP, EFC.	Multivariate encryption/decryption schemes are considered to be secure if they are protected against differential techniques, MinRank and algebraic attacks.
Multivariate public-key cryptosystem ^{234,237}	Multivariate public key cryptosystem, Rainbow signature scheme	In this system, public keys are a set of polynomial defined over a finite field. Infinite field, the degree of the polynomial is often considered as 2. Thus, it is referred to as multivariate-quadratic cryptography as well. Most of the multivariate public-key cryptosystems are quantum-resistant because no quantum algorithm solves the multivariate quadratic problem in polynomial time.

5.2.4 | Isogenies on super-singular-based cryptosystem

Cryptosystem-based on super-singular isogenies is an active area of research in post-quantum cryptography. The security of all supersingular isogeny cryptosystem schemes depends on the difficulty of computing the endomorphism ring of supersingular structures. Three popular isogeny-based structures used in post-quantum cryptography include ordinary isogeny Diffie-Hellman (OIDH), supersingular isogeny DH (SIDH), and commutative SIDH (CSIDH).²³⁸ Using these structures, the protocols in isogenies on the super-singular cryptosystems are majorly classified as signature/encryption, key exchange, and hash function. Isogeny-based digital signature schemes ensure message integrity, nonrepudiation, and identity authentication. The core idea of ensuring these cryptography properties is to transform identification schemes into signature schemes with non-interactive zero-knowledge proofs. The challenges in the signature can be generated using hash functions. In key exchange protocols, public and private keys are used to generate session key that ensures confidentiality and integrity of subsequent communications. The hash function ensures collision resistance and compression. The challenges that need to address in the future include the use of new quasi-linear algorithms for isogeny evaluations, optimization in the finite field arithmetics for isogenies, avoiding inversions using projective curve equations, and use other optimization approaches (like Montgomery forms). In attacks, isogenies on super-singular-based cryptosystems should consider the design of those cryptosystems that are well protected from ephemeral key recovery, active attacks (like protecting the long-term keys), and side-channel attacks. In Reference 239, the problem of endomorphism ring computation for supersingular elliptic curves is studied. This study is extended with an analysis of collision attacks over hash function parameters. The proposed directions to handle issues are generic in nature and can be extended for applications applying supersingular isogeny graphs. Thus, addressing Deuring's correspondence from maximal orders, or supersingular invariants can handle the preimage and collisions issues associated with a hash function or related parameters. In another scenario,²⁴⁰ the possibilities of power active attacks because of limited computing capabilities for the endomorphism ring of a supersingular elliptic curve are studied. In another major contribution, the factor involving partial knowledge in generating shared keys to determine the entire key is studied. This analysis is important to study side-channel attacks. Here, all forms of contributions are linked with computing capabilities. A higher computing

capability and partial knowledge of keys can exploit the supersingular isogeny curves. In Reference 241, an efficient commutative supersingular isogeny-based Fiat-Shamir signature algorithm is proposed. In this work, the large size of the public key is addressed by reducing it to half without affecting the security of the scheme. The proposed approach is tested against the quantum random oracle model and it is found to be secure for this scheme. Additionally, the proposed approach is found to be secure and effective compared to the existing approach in signing and verification. In verification, the challenge lies when there is a combination of the ephemeral key, secret key, and computational challenge. Thus, there is a need to address this challenge in the proposed scheme with fast, efficient, and security matters in consideration. In Reference 242, another quantum adversary resistant signature scheme is proposed and it is named as “Undeniable Blind Signature Scheme (UBSS).” Although it has been analyzed that the proposed scheme is hard to solve, it does not address the issue of combination. Addressing a combination of keys and challenges with a blind signature scheme is important to take up. In Reference 243, another blind signature scheme has been proposed. This scheme handles the undeniable signature issue in blind signature schemes. The proposed scheme is tested and found to be secure against various challenges. However, the issue of the combination of keys and challenges in the multi-party system needs to be taken up for further analysis. In References 243 and 244 the importance of hash function, challenges, and efficient approaches are proposed and discussed. For example, Doliskani et al.²⁴⁴ proposed a faster cryptographic hash function from supersingular isogeny graphs. The proposed approach provides exponential speed proportionate to characteristics of a finite field. The proposed approaches are claimed to be secure and less complex. However, an analysis against various active and side channel attacks can be conducted to work this work and ensure the security levels. Further, standard assumptions against whom the proposed approach is claimed to be secure should be used in comparative analysis with other similar work. The protocols in isogenies on the super-singular cryptosystem are briefly analyzed as shown in Table 11.

5.2.5 | Hybrid schemes

In hybrid schemes, different post-quantum cryptography primitives and protocols are integrated to achieve set goals. For example, Crockett et al.²⁴⁶ proposed a hybrid key exchange and authentication mechanism in Transport Layer Security (TLS) and Secure Shell Hash (SSH) protocols. The adoption of post-quantum cryptography with these mechanisms is found to be dependent on the standard of communication and availability of infrastructure. The integration of post-quantum and hybrid key exchange and authentication lies over the negotiation of multiple algorithms in hybrid cryptography that combine multiple keys and other primitives and protocols. The hybrid approach is found to be possible with the different hybrid key exchanges such as TLS 1.2, TLS 1.3, and SSHv2. Campagna and Crockett²⁴⁷ proposed the integration of independent key exchanges and feeding mechanisms with pseudorandom function (PRF) to drive

TABLE 11 Analysis of isogenies on the super-singular cryptosystem

Category	Variants	Major strengths
Isogeny-based signature/encryption algorithm ^{239–243}	SeaSign, CSI-FiSh, Quantum-resistant undeniable blind signature scheme, isogeny-based designated verifier blind signature scheme.	Lack of practices in the isogeny-based signature scheme makes this category of protocols weaker in post-quantum cryptography.
Isogeny-based key exchange protocol ²³⁹	Longa, LeGrow, Galbraith, Authenticated Key Exchange (AKE)-SIDH-2, AKE-SIDH-3, SIDH-UM, biclique-SIDH.	The major challenge in key exchange protocol is to design authenticated key exchange protocol and verify the security with well-known security models such as BR, CK, CK ⁺ .
Isogeny-based hash function ^{244,245}	CGL, Very Smooth Hash (VSH), VSH-DL, SWIFFT, Takashima’s hash function, Charles, Goren and Lauter’s hash function.	High-speed isogeny-based Hash functions are protected from Pollard-rho, claw finding, preimage, and collision-resistant attacks. High-speed short messages-based Hash functions are useful to avoid quantum attacks of computational overhead that are used with novel solutions.

a secret and secure exchange. In this work, a new hybrid key exchange mechanism is designed for TLS 1.2 protocol with elliptic curve Diffie-Hellman protocol and post-quantum key encapsulation. Further, Bit Flipping Key Exchange (BFKE) and Supersingular Isogeny Key Exchange (SIKE) are combined with the key exchange in TLS 1.2 handshake mechanism. Overall, the integration is found to be effective, and desired goals are achievable with good performance measures. Qassim et al.¹⁵⁵ combined physical layer and cryptography security primitives for increasing the security standard and proposed a cross-layer key agreement scheme that is strongly protected against a man-in-the-middle attack. This technique is found to be unbreakable and scalable to traditional cryptography primitives and protocols.

6 | SCALABLE QUANTUM COMPUTER HARDWARE

As a full-fledged field, experimental QC started as early as the 1980s, however, until the late 1990s, the majority of the researcher's envisaged industrial quantum computer as a distant reality.³ Several contenders have attempted to create building blocks of a scalable quantum computer and they are developed independently by different academic researchers and industry engineers worldwide. For the design and implementation of qubits and quantum gates, a number of candidate material systems are being investigated. Some of the front-runner material systems include trapped ions,¹⁰ optical lattices,¹² solid-state spins,¹¹ electron spins in gated quantum dots,²⁴⁸ quantum wells,²⁴⁹ quantum wire,²⁵⁰ nuclear magnetic resonance (NMR),²⁵¹ solid-state NMR,²⁵² molecular magnet,²⁵³ cavity quantum electrodynamics,²⁵⁴ linear optics,²⁵⁵ diamond,²⁵⁶ Bose-Einstein condensate,²⁵⁷ rare-earth-metal-ion-doped inorganic crystal,²⁵⁸ and metallic-like carbon nanospheres,²⁵⁹ among others. However, superconducting circuits have transpired as the most widely used and successful material system to-date, although trapped ion system is also demonstrating excellent qubit fidelities and gate times.

The two main approaches for the physical implementation of a quantum computer are analog and digital.²⁶⁰ A significant challenge for the construction of error-free industrial quantum computers is the maintenance of qubit state due to decoherence. Even with error rates achieved below 1%, the depth of quantum circuits required to solve real-world problems would be considerable, leading to detrimental cumulative error rates. Therefore, the area of quantum error correction is at present one of the most active areas of the research. Google Quantum AI, in collaboration with NASA, reported a demonstration of quantum calculation which was shown to require several 1000 years on any conventional classical computer on October 23, 2019. Although this work achieved an important milestone for the current generation of quantum computers, the solution of a practical real-world problem on a quantum computer is expected to require significant further development. Notably, the work from IBM researchers showed that the efficiency of the same calculation on a classical supercomputer can be significantly improved.²⁶¹

6.1 | Quantum computers and speed-up

Quantum computers can solve the certain computationally intense tasks in significantly less time compared to classical computers, which is shown by the demonstrated "quantum supremacy." Another important term commonly used in the quantum community is "quantum advantage." While "quantum supremacy" implies solving a problem on a quantum computer which is intractable on any classical machine; whereas "quantum advantage" is a more practical term which deals with solving a useful real-world problem which cannot be efficiently solved on a classical computer. Although quantum supremacy has already been demonstrated, it is yet an open area of research to find practical problems which can be efficiently solved on quantum computers.

The quantum machines that have been engineered hitherto are bulky and offers limited computational power as they are made up of materials which have to be kept at superconducting temperatures, nevertheless, the potential of industrial quantum computers in future cannot be contested.²⁶⁰ The motivation for potential benefits of industrial quantum computers can be derived from the present-day success of classical computers and the way they took off in the 1950s. Similar to the practical state of quantum computers today, the first generation of classical computers used to be bulky and had to be cooled continuously. As the theory of artificial intelligence (AI) had started shaping from the early days of classical computers, albeit they were nowhere near the compute required

for AI, powerful industrial quantum computers can be theorized to come to reality in near-future and achieve “quantum advantage.”

6.2 | Industrial applications of quantum computers

Cryptanalysis is an inquiry into the information systems to determine the secret aspects of the system. It is used to circumvent the cryptographic safety mechanisms to access the contents of encrypted messages. An example is the RSA (Rivest–Shamir–Adleman) encryption which is widely used for encrypting data communication with banks and other nodes on the internet. Shor developed a quantum algorithm in 1994 which can, in principle break the operational RSA encryption if a large-scale error-corrected quantum computer can be developed. Hence, post-quantum encryption methods need to be formulated which can withstand an industrial quantum computer.⁴⁹ Searching efficiently and sorting through large data sets is now a high priority for many big enterprises. Grover developed an optimal quantum algorithm in 1996, which can speed up search through big data relative to the classical algorithms in query complexity. The present-day database software’s such as Oracle are not suitable enough for real-world search enough to run Grover’s algorithm; hence software that does the work of oracle in the quantum world need to be developed.⁵⁰

A variety of areas in computational sciences such as numerical weather prediction, computational chemistry and others involve solving equations using approximate methods ignoring the fine details. An example is the parameterization techniques used to approximate the sub-grid scale processes in a weather/climate prediction model due to the computational constraints. These approximate parameterizations have been known to propagate errors in the solutions to the system of equations, thus directly affecting the decision making. Industrial quantum computers offer hope in solving the equations in their exact form. This could for example allow an understanding of how different chemicals make fertilizers and improve upon the current high carbon footprint technique of manufacturing. Understanding chemistry, photosynthesis, superconductivity and magnetism, all being quantum mechanical phenomena can be better understood by industrial quantum computers. Although a scalable industrial quantum computer has still not been achieved and may require significant further development, research at the proof-of-concept level has started using the available, relatively less powerful quantum computers. On a seven-qubit quantum processor, IBM recently simulated beryllium hydride molecule.²⁶² Various applications such as patient diagnosis by quickly comparing the reports with a global database, modeling of live passenger and commercial traffic, the balance of energy supply and demand are expected to gain traction in the next few years. On the other hand, several other areas such as encryption, communications, financial transactions, critical infrastructure, Blockchain, and cryptocurrency are some of the applications which are bound to become vulnerable by the development of an industrial quantum computer.

6.3 | Hardware requirements of industrial quantum computers

International efforts on how to build, construct, and monitor qubit systems by over 100 academic and government-affiliated labs are underway. A number of large corporations and numerous ambitious start-up companies are now working on manufacturing of industrial quantum computers. Beside the development of qubits and quantum gates, an industrial quantum computer would also require intricate classical control and circuitry such as the application of electromagnetic fields, cooling system, user interface, networks, and data storage capabilities. The hardware requirements of industrial quantum computers can be divided into four layers based upon their functions, namely, the “quantum data plane,” the “control and measurement plane,” the “control processor plane,” and the “host processor.” The “quantum data plane” is the location where qubit states are stored and measurements are carried out by the “control and measurement plane.” The sequence of operations in algorithms is taken care of by the “control processor plane,” and the “host processor” carries out the user interface, networks and storage of large arrays.

6.4 | Challenges in scalable production of industrial quantum computers

In order to build a functional industrial grade quantum computer, several technological issues have to be addressed; the most important of which being the detrimental impact of noise or decoherence which causes errors in quantum computation and suppresses quantum advantage. An initial state of a qubit has to be set before it can be used in addition

TABLE 12 Major hardware candidates for industrial quantum computer and their properties

Qubit technologies	Trapped ion qubits²⁶⁵	Superconducting qubits²⁶⁶	Silicon qubits²⁶⁷	Photonic qubits²⁶⁸	Topological qubits²⁶⁹
Physical qubits	IonQ:79; AQT:20	IBM: 65 qubits; Google: 54 qubits; Rigetti: 30	2	6×3^9	In progress
Coherence times	~50 s	~50–200 μ s	~1–10 s	~150 μ s	–
Gate fidelity	~99.9%	~99.4%	~90%	~98%	Expected: ~99.9999%
Gate operation time	~3–50 μ s	~10–50 ns	~1 ns	~1–10 ns	–
Scalability	Some potential	Medium to high potential	High potential	High potential	–

to developing circuits and gates. Photons remain coherent for a long time; however, creating quantum circuits out of them is a challenge. Superconductors possess quantum properties which can be harnessed to develop quantum circuits which are in use by IBM, Google, Rigetti, and others to build their quantum computers. However, the fidelity of these qubits, in particular of two-qubit operations, is still relatively low and therefore require error correction or mitigation techniques to be implemented. In 2016, IBM released a five-qubit processor free for everyone on the cloud, which can be used to construct a quantum circuit and run it as long as it uses five or fewer qubits.²⁶³ At present, IBM offers cloud access to quantum computers consisting of up to 65 qubits and has recently announced a quantum computer with a record 64 quantum volume.²⁶⁴

Table 12 shows five major candidate material systems for the development of an industrial quantum computer and the relevant metrics to measure their performance and the current state-of-the-art. Among these candidate systems, trapped ion and superconducting qubits are the basis for the current generation of quantum machines available through cloud access. The other three material systems are still a subject of intense research and require significant further development to be available for quantum circuit simulations.²⁷⁰ Although there has been much progress in designing smaller quantum computers, it is not yet possible to experimentally demonstrate a design for an industrial quantum computer which could be of the scale required to crack current cryptography and the existing implementations even if scaled up are not just enough. Scaling the qubits to achieve an industrial quantum computer has many challenges such as the quality of qubits when scaling up to industrial-scale quantum computers, wiring, refrigeration, packaging, and others.

Theoretically, silicon-based quantum computers have been predicted to offer the potential for scalability with error correction schemes. After the seminal work from Kane in 1998,²⁵² many surface-code quantum computer architectures have been proposed.^{271–273} Remarkable advancements in silicon spin qubit design and characterization^{274–279} demonstrated in the recent years, confirm the suitability of this material system as an attractive candidate for the construction of a scalable industrial quantum computer.

6.5 | Currently available platforms

IBM released the quantum computer known as IBM Quantum Experience in 2016 which was a five-qubit system. The system was launched with a user guide and a community forum. Later in 2017, a number of features were added to IBM Quantum Experience such as giving permissions to the users to interact via quantum assembly language, interactive use interface and simulator expansion. IBM then launched Qiskit which helped to code on the quantum processor. Further they developed a 16-qubit system and also launched the quantum awards program. The Quantum Experience is a cloud-computing based platform which provides access to the public to the quantum processors, an online forum and the tutorials to code on Q devices of IBM. Various research publications have used the IBM Quantum Experience. The hardware of quantum processors by IM is superconducting qubits which reside inside a dilution refrigerator. The GUI that users interact with is known as the quantum composer. Quantum composer is used to write quantum assembly code. The GUI facilitates the development of quantum experiments and algorithms. The option to use a real processor or a simulator is also available.

A similar cloud-based QC service is provided by Rigetti Computing through its platform known as Forest. The company is primarily known for manufacturing quantum integrated circuits. Forest helps the coders to access the cloud-based quantum processors by Rigetti wherein they can test their quantum algorithms. They have also developed a dedicated

quantum instruction language called Quil which is used for the cloud-based QC as a service. More than 36 qubits are available on a quantum chip of Forest and Python programming can be used for hybrid classical or QC. Quantum Inspire is a Europe based cloud-computing based quantum platform which is providing its services under the name of a company known as QuTech. The cloud-based QC systems offer access to the power of QC and simulate quantum algorithms without the need of buying or building a quantum computer.

6.6 | State-of-the-art and future outlook in industrial quantum computers

The size of the industrial QC market is expected to touch \$1.9 bn by 2023 and \$8 bn by 2027.²⁸⁰ Various computing giants such as IBM, Microsoft, Alibaba, and Google dedicated quantum enterprises such as D-Wave and others such as Rigetti Computing and NVision Imaging Technologies are testing quantum computers competing to launch the scalable industrial computer. Global research and development efforts are ongoing to commercialize industrial quantum computers with continuously increasingly leading contributions from United States and other prominent efforts coming from the EU quantum technologies flagship and the UK national quantum technologies program, the Australian Centre for Quantum Computation and Communication Technology (CQC2T) and the Chinese quantum national laboratory for quantum information science.

6.7 | Blind quantum computation

Blind quantum computation (BQC) ensures infrastructure to do quantum computations while hiding from the server the computational structure. In addition to privacy protection, many BQC techniques incorporate embedded control tests that check the computation process. BQC allows us to do calculations without revealing the calculation results to anybody. In BQC, the encryption protocol safeguards computational inputs, outputs, and algorithms.^{281–283} Homomorphic encryption encrypts inputs and outputs only. Thus, BQC is more secure than homomorphic encryption. Figure 12 shows the important terminologies associated with BQC. Some of the important concepts related to BQC are briefly explained as follows:

- Universal blind quantum computation: UBQC protocols permit the client to create random states from a finite set. These states are used to ensure secure delegation of quantum computational tasks to a server. UBQC protocol consists of four phases, including pre-computation (for angles measurement and unitary computation from brickwork state), Alice's preparation (qubits computation), Bob's preparation (brickwork state computation), and interaction and

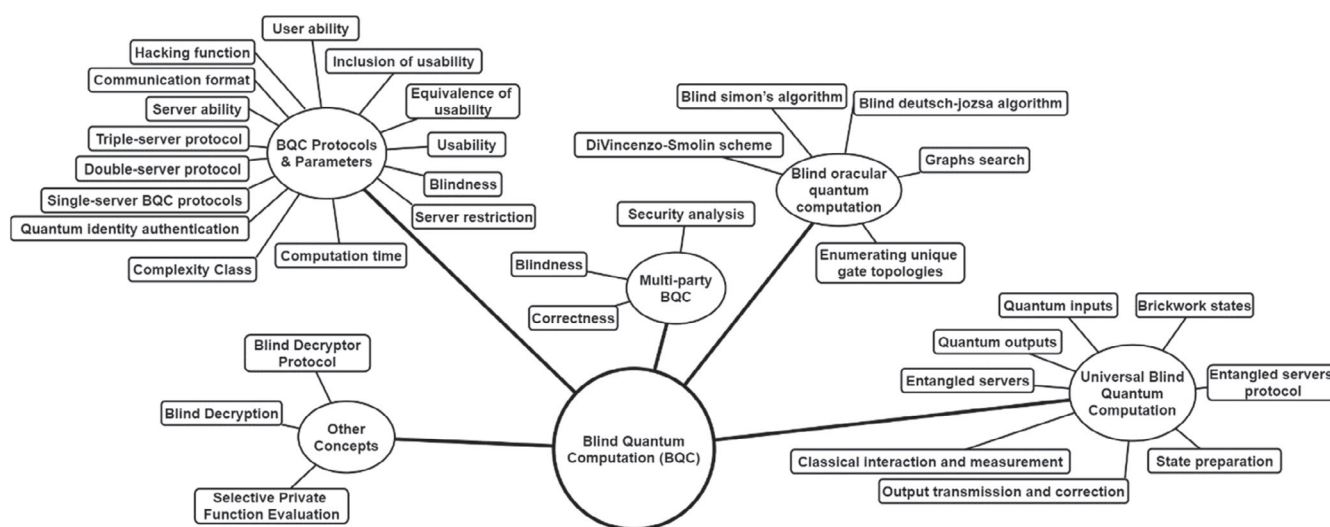


FIGURE 12 Blind quantum computation and taxonomy

measurement (angle measurement, angle encoding, and verification process). The performance of protocol is measured using correctness, universality, and security.

- **Blind oracular quantum computation (BOQC):** In BOQC, a third party executes the client's oracular quantum computations on a server. Here, third-party support is considered because the client is assumed to have limited quantum power and capacity to construct an oracle. Third-party identifies a server that can take the help of an oracle to do the required computations. Gustiani and Bandung²⁸⁴ surveyed important concepts, protocols, and terminologies associated with BOQC in the quantum era.
- **BQC protocols and parameters:** In addition to BQC, UBQC, and BOQC, various protocols and parameters are associated with BQC. For example, single-server BQC protocols, double-server protocol, triple-server protocol, and so forth. Figure 12 shows the classification of important protocols and parameters in the BQC area.^{281–283}

7 | FUTURE DIRECTIONS

We have identified various ongoing research areas in QC for three different maturity levels (5 years, 5–10 years, and more than 10 years) based on the state-of-the-art research. They are illustrated in Figure 8 as the hype cycle for QC. *T* represents technology, and *A* means the application area in the hype cycle. As per Figure 13, post-quantum cryptography is at the peak while a lot of research work has been done on simulations for complex quantum experiments. Research areas such as robotics, energy management, cybersecurity, distributed QC, complex computational chemistry, financial modeling, and drug design are at the kickoff stage in their development under the domain of QC. The use of QC in these areas at their innovation trigger, may take more than 10 years to mature. Traffic optimization is also at its innovation trigger but is expected to top the hype cycle within the next 5–10 years. Quantum cryptography, quantum control, and adiabatic QC have peaked inflated expectations. It is expected that it would take less than 5 years for them under complete development under QC purview. Quantum Internet, quantum-based satellite communication, quantum assisted machine learning, electronics material discovery, and error-corrected QC have also reached the peak of inflated expectations but are anticipated to rapidly evolve in 5–10 years. Quantum based portfolio-risk optimization and fraud detection, and fault-tolerant

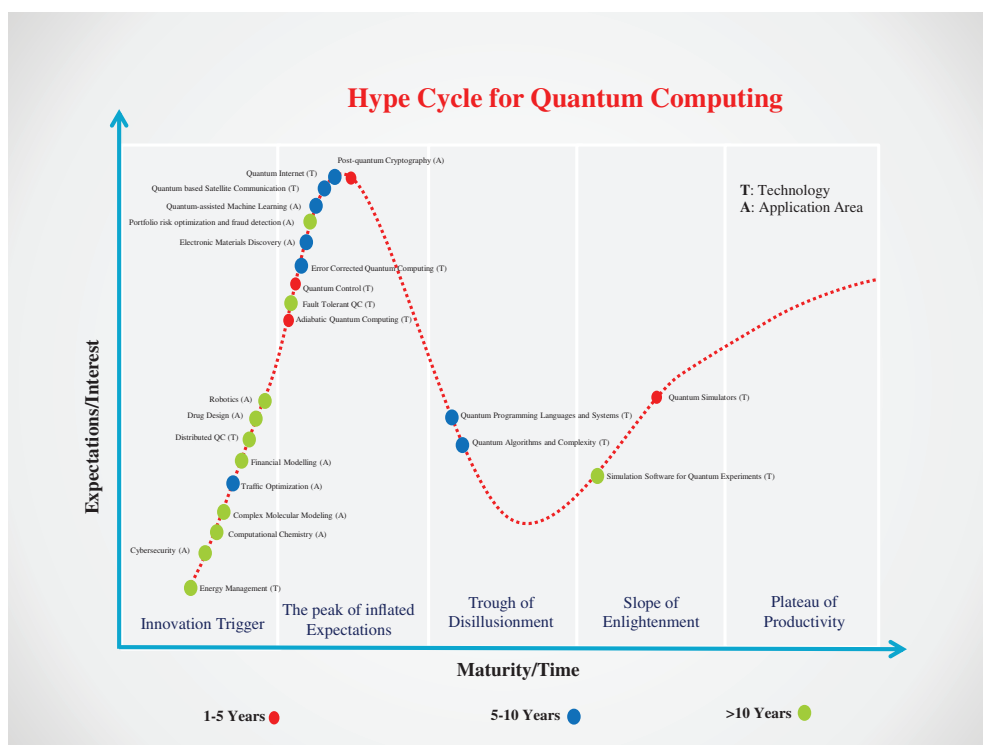


FIGURE 13 Hype cycle for quantum computing

QC presently have high expectations on the hype cycle and are blossom in more than 10 years. A lot of research work has been done on quantum algorithms and complexity, and quantum programming languages and systems, which could be active research areas during the next 5–10 years. Simulation software for quantum experiments and quantum simulators is at the enlightenment slope and has a long way to develop in QC fully. We have identified various open challenges and future research directions, which are still a topic of active global research.

7.1 | Engineering/design challenges

Fragility is the main drawback of Quantum technology due to two following reasons²⁸⁵: (1) A short coherence time of qubits because superconducting qubits forget their information very frequently (in nanoseconds). (2) There is unreliability in quantum operations due to relatively large error rates, and it is challenging to develop a quantum computer with low error rates. Moreover, small material faults or environmental instabilities can generate an error in qubits and lose their quantum data, which reduces the useful period of a qubit. There is also need to perform logical functions while controlling the qubit to reduce incidental electromagnetic noise, which can decrease decoherence. To improve the scalability of the quantum computers, balance is required among protecting qubits from prospective environmental instabilities. Further, as compared to classical computing, error correction in QC is quite challenging because (a) errors are continuous (involves both amplitude and phase), (b) cannot copy unidentified quantum states, and (c) measurement can collapse a quantum state and destroy the data saved in qubits. To run a quantum algorithm efficiently, many physical qubits are required, which need a close and continuous connection between the classical platform and quantum chip, and it forms a colossal control overhead.²⁸⁶ Moreover, this interaction and overhead increases the complexity for QC process in terms of run-time control, architecture and integration. Currently, qubit count is using to measure the power in QC hardware. Still, this measure is not giving correct value and leads to the challenge of the power of future powerful quantum computers with more than 1000 qubits. Qubit architecture improves scaling to solve the dynamic sized complex problems, but it needs an efficient cooling component to maintain heat, which can be solved by utilizing AI-empowered systems.

7.2 | Reliable QC

It is challenging to attain fault-tolerant and reliable quantum computations as practical implementation of quantum error correction is still an open problem.²⁸⁷ Due to quantum states' delicate nature, there is a need to operate bits at very low temperatures, and fabrication should be highly accurate.²⁸⁸ It is also challenging to measure complete quantum state accurately; therefore, verification is challenging. There is a significant probability of errors during computation as compared to classical computing. There is a need for an effective error correction mechanism for quantum architectures to operate as intended. There is also a need to redesign quantum communication architecture to increase the verification of precise fabrication constraints. On the other hand, qubits are very difficult to test after fabrication because tolerances are tight, and the use of incorrectly placed qubits must be avoided to reduce the occurrence of error. There is a need to apply error correction recursively to attain adequate fault tolerance to permit sustainable quantum computation.²⁸⁹ In future, the latest AI and ML-based techniques can be used for automatic detection and corrections of errors dynamically to offer valuable and reliable service. The utilization of recent AI and ML-based techniques can improve the reliability but it can also increase the complexity within the system by increasing the processing of data, which leads to extra training cost for AI/ML techniques as well.

7.3 | Quantum-assisted machine learning

Machine learning researchers use principal component analysis, vector quantization, Gaussian models, regression, and classification in routine.²⁹⁰ To improve the scalability and efficiency of machine learning algorithms, quantum technology can be used in handling large datasets with large sizes of devices (100–1000 qubits).²⁹¹ Further, quantum computers can efficiently attract the interest of the machine learning community by preparing and sampling definite probability distributions efficiently, such as training in classical and quantum generative models. Nowadays, the input size (the number of users) for the quantum recommendation system algorithms is increasing, which is challenging to complete the

operation with the required speed. There is a need for millions of qubits to handle the current demand and tackle large datasets. The hybrid quantum-classical algorithms can solve this problem by providing current computation power and other machine learning tasks.²⁹¹ The other essential challenges can be limited qubit connectivity, and the device's integral noise increases decoherence in the qubits. The utilization of advanced AI and reinforcement learning can increase the scalability and offer more computational power to handle a vast amount of data generated from various IoT devices.²⁹² Further, NISQ devices with the viewpoint of tensor networks can be used to explore the workflow of quantum-assisted machine learning, which can provide a healthy platform to develop innovative ML models to improve the resource management within the quantum computer. The effective management of resources can also reduce the impact of the noise fluctuations on the performance of quantum hardware.

7.4 | Energy management

Energy management is a significant challenge, where the world's powerful supercomputers and cloud data centers consume a lot of energy to solve different problems.²⁹³ Quantum computers are expected to be more energy-efficient than them (supercomputers/data centers) while executing a particular task.²⁹⁴ On the other hand, a quantum computer can reliably perform extensive calculations using less energy, which further reduces the cost and carbon emissions. Classical computers use binary bits (0 or 1) for encoding information, while QC uses qubits, which represent both 0s and 1s simultaneously—this property of QC to identify an optimal solution while consuming less energy. The reason for less energy consumption is that the quantum processors are working at shallow temperature, and the processor is superconducting with no resistance, which means no production of heat.²⁹⁰ Hybrid applications contain two portions: high-energy and low-energy.²⁹³ QC executes the high-energy portion, while classical computing executes the low-energy part using the cloud.²⁹⁵ To solve these kinds of problems, there is a need for hybrid computing comprised of quantum and classical computing to curb energy usage and costs dramatically. There is a need to do more work before implementing hybrid computing to solve today's most challenging business problems. Quantum computers can use AI to improve computational speed, reliability, and security and increase the size of infrastructure, which needs a vast amount of energy to run it and control the temperature using cooling devices. In future, the energy demand of these Quantum computers can be fulfilled with the utilization of renewable energy along with brown power. Further, the energy demand of quantum computers can be predicted using latest machine learning techniques to estimate the demand of both renewable and non-renewable energy. Further, effective data analytics techniques can be utilized to perform accurate predictive analytics for energy consumption. The quantum computers need to be scaled up from 50 qubit systems to the 10,000 for solving the complex problems of computational chemistry and biology, which needs more energy for computing and cooling (to maintain the temperature). So, there is a need to develop the energy-efficient quantum data centers for better utilization of energy.

7.5 | Quantum Internet

Quantum Internet enables distributed QC by incorporating new communications and improving computing capabilities to a large extent. Quantum Internet has various challenges because it uses quantum mechanics laws, and the main constraints for network design are teleporting, entanglement, quantum measurement and no-cloning.²⁹⁶ The error-control mechanism is an essential assumption of classical computing, which is no more valid in QC. There is a need for a major shift in network paradigm from classical to quantum specific to the design quantum Internet. Further, when a qubit interacts with an environment, it causes decoherence because qubits are fragile and lose information from qubit to the environment over time. Moreover, the long-distance entanglement distribution is also a challenge in QC for the effective transformation of data. To improve the computation and communication mechanisms within quantum computer nowadays needs a large amount of memory which would be more challenging with future quantum Internet to retain the details of operations performed. Further, there is need of high bandwidth to offer effective communication among quantum devices, computers and web applications. It would be also challenging to make the current web applications compatible with quantum Internet applications depend on entangled qubits. So, there is a need of uniform interface which allow quantum sensors, quantum computers and quantum Internet applications can exchange data using quantum Internet.

7.6 | Robotics

Robots use GPUs to solve intensive computational tasks such as drug discovery, logistics, cryptography, and finance, where QC can be augmented to perform computations with a considerable speed. Quantum-powered robots can also utilize cloud-based QC services to solve different types of problems.²⁹⁷ Nowadays, QC enhances robotic senses for manufacturing, such as identifying several faults in a jet engine in a short period.²⁹⁸ Further, quantum image processing helps to understand the visual information efficiently and saves and manages image data effectively using two critical QC properties such as parallelism and entanglement. AI-based robotics are dealing with different kinds of problems using graph search to deduct new information, but complexity increases with the increase in data. QC can reduce complexity by using quantum random walks instead of graph search. Further, other significant problems related to kinematics, such as the mechanical movement of robotics, can be solved by quantum neural networks by enhancing machines' activity and recognizing moments of joint friction and inertia. Moreover, another problem, such as identifying the reason for the inconsistency between expected and observed behavior, is challenging, which could be solved using quantum algorithms. QC uses to optimize the motion of machines in robotics, such as joint friction and moments of inertia, which can be solved by quantum reinforcement learning in the future. The utilization of quantum processor is improving the automatic learning process in robotics using superposition principle but it is also increasing complexities within the system. Further, it will also increase the cost of building quantum technology based robots due to training and learning expenses of machine learning models.

7.7 | Simulations for complex quantum experiments

QC can simulate complex chemistry, physics, and biology problems using small-scale (50–100 qubit) “quantum simulators,” which could be available in coming years.²⁹⁹ The expertise of an extensive range of researchers and fundamental aspects of classical computing can work together to understand and harness quantum technology's capabilities. Further, quantum simulators can realize the natural system while solving complex problems (which is difficult to solve on the classical system or supercomputer) in a controlled manner to measure the influence of various parameters on each other. Quantum simulators can take advantage of QC's essential properties such as entanglement and superposition while designing it. There is a need to develop large-scale programmable quantum system for effective processing of information for complex processes in chemistry and physics. In future, more scalable systems or simulators can be developed to run large-sized and complex jobs related to chemistry and biology with optimum results by investigating the hardware-efficient realization of quantum algorithms.

7.8 | Post-quantum cryptography

There is a need for cryptography to improve the security for implanted medical devices, cares, and online communication. Nevertheless, the various generally used cryptosystems will be damaged once large quantum computers come into existence. Post-quantum cryptography denotes the cryptographic algorithms (generally public-key algorithms). It is assumed that the attacker used a large quantum computer to attack in post-quantum cryptography, and these systems attempt to stay secure in this situation.⁵⁴ Post-quantum cryptography has to maintain integrity and confidentiality while preventing different kinds of attacks. Post-quantum cryptography research is typically concentrated on six techniques such as symmetric key quantum resistance, supersingular elliptic curve isogeny cryptography, code-based cryptography, hash-based cryptography, multivariate cryptography and lattice-based cryptography.³⁰⁰ Another challenge within post-quantum cryptography is “agility”; there is a need to find out the right areas to incorporate agility. Therefore, future systems should build in such a way, which must be able to predict the possible security problems. Further, there is a need for testing and validation design by developing new automated tools to identify and fix the fault at runtime dynamically. Moreover, the reconfiguration of legacy devices with cryptosystems is still an open problem, which needs to be solved by incorporating agility in the legacy applications. Future works need to explore more secure code-based systems that give outcomes at a lesser cost of delay. Thus, trade-offs between delay, security, and information rate need to be studied in detail. High computational and communicational rates without scarifying security are the aim. To adapt to post-quantum cryptography transition in real-time applications, there is a need to formalize a wide array of standards. For example, integration with banking, remote learning, mobile communications, healthcare, and other emergency services, and

critical infrastructure requires studying post-quantum algorithm choices. The selection of these algorithms can speed up the migration process as well. Quantum computers can use QKD and integrates verifiable quantum key generation with quantum-safe cryptosystems (multivariate constructions, lattice-based, isogeny-based, hash-based and code-based) to provide the unbreakable security but it would be expensive. Another non-expensive solution could be hybrid implementations (pre-quantum and post-quantum schemes), which can also be used to improve the data privacy from quantum capable attacker.

7.9 | Numerical weather prediction

The development of classical computers was accompanied by advancements in numerical weather prediction skills in the 1950s. Since then, the predictions of weather forecasts have greatly enhanced in the last few decades. This development has been catapulted by the improved hardware and software but has been limited by the fundamental principle on which these traditional computers are built, that is, bits or 0s and 1s. For the purpose of colossal calculations required, the classical computers are stacked to build what are known as supercomputers. These supercomputers perform computations day and night to generate forecasts of the atmosphere, ocean, land, and other components of the Earth system. Although they have improved with time, the state-of-the-art predictions still need a lot of upgrades for societal applications such as flood forecasting, urban modeling, sub-surface flow modeling, and allied complex tasks. These developments have been limited by the computational power available today. With the hope of industrial quantum computers becoming a reality, the next-generation Earth System Models would be able to run at much higher spatial and temporal resolutions. There is a need to diligently study QC's applicability to numerical weather predictions.³⁰¹ Numerical weather prediction can adopt QC because the limitations of classical computing lead to erroneous high-resolution forecasts. The scientific goal is partial differential equations on the three-dimensional spherical atmosphere and ocean, which is limited in the spatial resolution by the computational power of classical computers. QC can tackle the important challenges of climate change such as global warming and the production of CO₂ emissions. Further, weather and climate models can be simulated using quantum technology based large scale simulators to determine different catalysts for carbon capture in a cost-effective manner.

7.10 | Quantum cloud computing and cryptography

An unconditional secure quantum cloud computing can be a major ingredient to various real-life applications if powerful quantum computers will become widely available in future.³⁰² A few powerful quantum-computer nodes in a cloud would make the client's job much easier. Client would need to communicate with quantum clouds via a quantum link for transferring their job and associated qubits. The efforts have been made in this direction to experimentally demonstrate blind QC where input, delegation, computations and output are unknown to quantum servers. These developments have been limited by the universal and powerful quantum clusters. Cryptographic verification of quantum cloud computing, fault-tolerant secure quantum computations, error-free quantum cryptography mechanisms, cryptography primitives, and key distribution mechanisms in quantum cloud computing environment, and quantum techniques for access control in cloud computing.^{303–306} In conclusion, secure and efficient quantum cloud computing environment is required to be studied in-depth for universal QC at large scale. Further, cloud-based environment will be an effective approach for storage, computation and distribution of data to the QC community. In these systems, latency and network bandwidth can be challenges for the execution of small jobs, which can be solved using the concept of fog/edge computing. To provide the quantum as a cloud service, there is a need of large scale systems which can offer autoscaling. Serverless computing can be used to offer the dynamic scalability to solve the complex problems along with quantum technology. The latest security mechanism such as Blockchain can be used to provide more secure and reliable service. Further, the integration of Blockchain service with Quantum Internet can improve the communication speed along with required security.

8 | SUMMARY AND CONCLUSIONS

This article presents a systematic review of QC literature. It identified that quantum-mechanical phenomena such as entanglement and superposition are expected to play an important role while solving computational problems. We

proposed a taxonomy of QC and mapped it to various related studies to identify the research gaps. Various quantum software tools and technologies are discussed. Further, post-quantum cryptography and industrial quantum computers are discussed. Various open challenges are identified, and promising future directions are proposed. The fusion of all the performance attributes in a single QC technique is still ambiguous until now. To build a quantum computer which can perform concurrent operations, it is essential to have a QC technique that can allow quantum I/O with all the necessary classified features. The suggested taxonomies framework can be used to contrast various existing QC techniques for determining the optimal strategy that can be applied on classical computing infrastructure. However, the scaling of qubits, trade-off between speed and the decoherence time is the topic of research in the field of QC.

Quantum computers are developed to increase the security rate in communication and computations via decreasing the computational time. To secure the classical cryptography primitives and protocols with the usage of quantum computer's ability in solving the mathematical problems in few milliseconds, post-quantum cryptography mechanisms are designed. Post-quantum cryptography strengthens the symmetric cryptography primitives and protocols against well-known quantum attacks. Further, it has taken three hard mathematical problems (integer factorization, discrete logarithmic, and elliptic-curve discrete logarithm) in asymmetric key cryptography to secure the cryptography primitives and protocols. In conclusion, the characteristics of post-quantum cryptography increase the computational efficiency and security of many futuristic applications.


Furthermore, the present-day industrial quantum computers are not yet there to replace classical supercomputers owing to the challenges in scaling up on the number of qubits that can be practically realized hitherto. When that might happen is an open question. Though the next decade is going to be highly exciting for industrial quantum computers, there is still uncertainty on when the quantum computers will start to replace their classical counterparts in complex tasks. However, digital supercomputers are here to stay, even if quantum becomes a reality, as an addendum to the quantum computers of the future.


There is one crucial design challenge: how to run a quantum algorithm efficiently? A large number of physical qubits are required, which need a close and continuous connection between the classical platform and quantum chip, forming a huge control overhead. It is challenging to achieve fault-tolerant and reliable quantum computations because of quantum error correction, which is still an open problem. Due to the fragile nature of quantum states, there is a need to operate bits at very low temperatures and fabrication should be accurate. Further, to improve the scalability and efficiency of machine learning algorithms, quantum technology can be used in handling a large dataset with a large number of devices (100–1000 qubits). Energy management is a research area in the field of QC. To improve energy efficiency, there is a need for hybrid computing comprises of quantum and classical computing to curb energy usage and costs dramatically. There is a need to do more work before implementing hybrid computing practically to solve today's hardest business problems. Quantum simulators can be designed for simulations for complex quantum experiments, which can take advantage of important properties of QC such as entanglement and superposition while designing it. Presently, AI based robotics are dealing with different kinds of problems using graph search to deduct new information, but complexity is increasing with the increase in data. QC can reduce the complexity of robotic mechanism by using quantum random walks instead of graph search. Other various fields such as computer security, biomedicine, the development of new materials and the economy will benefit from the advancement in QC.

DATA AVAILABILITY STATEMENT

Data sharing not applicable to this article as no datasets were generated or analyzed during the current study.

ORCID

Sukhpal Singh Gill  <https://orcid.org/0000-0002-3913-0369>


Adarsh Kumar  <https://orcid.org/0000-0003-2919-6302>

Harvinder Singh  <https://orcid.org/0000-0002-9427-1279>

Manmeet Singh  <https://orcid.org/0000-0002-3374-7149>

Kamalpreet Kaur  <https://orcid.org/0000-0001-7162-2059>

Muhammad Usman  <https://orcid.org/0000-0003-3476-2348>

Rajkumar Buyya  <https://orcid.org/0000-0001-9754-6496>

REFERENCES

1. Feynman RP. Simulating physics with computers. *Int J Theor Phys*. 1982;21(6/7):467-488.
2. Preskill J. Quantum computing and the entanglement frontier; 2012. arXiv:1203.5813.

3. Preskill J. Quantum computing in the NISQ era and beyond. *Quantum*. 2018;2:79.
4. Ball P. Google moves closer to a universal quantum computer. *Nature News*; 2016. Google moves closer to a universal quantum computer.
5. Quantum Algorithm Zoo. <http://quantumalgorithmzoo.org/>
6. Zhang DB, Yuan ZH, Yin T. Variational quantum eigensolvers by variance minimization; 2020. arXiv:2006.15781.
7. Lloyd S, Mohseni M, Rebentrost P. Quantum principal component analysis. *Nat Phys*. 2014;10(9):631-633.
8. Cong I, Choi S, Lukin MD. Quantum convolutional neural networks. *Nat Phys*. 2019;15(12):1273-1278.
9. Devitt SJ. Classical control of large-scale quantum computers. *Proceedings of the International Conference on Reversible Computation*; 2014:26-39; Springer, Cham.
10. Paul W. Electromagnetic traps for charged and neutral particles. *Rev Mod Phys*. 1990;62(3):531-540.
11. Imamog A, Awschalom DD, Burkard G, et al. Quantum information processing using quantum dot spins and cavity QED. *Phys Rev Lett*. 1999;83(20):4204-4207.
12. Grimm R, Weidemüller M, Ovchinnikov YB. Optical dipole traps for neutral atoms. In: Berman PR, Lin CC, Arimondo E, eds. *Advances in Atomic, Molecular, and Optical Physics*. Vol 42. Academic Press; 2000:95-170.
13. Fedichkin L, Yanchenko M, Valiev KA. Novel coherent quantum bit using spatial quantization levels in semiconductor quantum dot; 2000. arXiv quant-ph/0006097.
14. Giovannetti V, Lloyd S, Maccone L. Quantum random access memory. *Phys Rev Lett*. 2008;100:160501.
15. Harrow AW. Small quantum computers and large classical data sets; 2020. arXiv preprint arXiv:2004.00026.
16. Cortese JA, Braje TM. Loading classical data into a quantum computer; 2018. arXiv preprint arXiv:1803.01958.
17. Savchuk MM, Fesenko AV. Quantum computing: survey and analysis. *Cybern Syst Anal*. 2019;55(1):10-21. <https://doi.org/10.1007/s10559-019-00107-w>
18. Gyongyosi L, Imre S. A survey on quantum computing technology. *Comput Sci Rev*. 2019;31:51-71. <https://doi.org/10.1016/j.cosrev.2018.11.002>
19. Brass D, Erdélyi G, Meyer T, Riege T, Rothe J. Quantum cryptography: a survey. *ACM Comput Surv*. 2007;39(2):6.
20. Abura'ed N, Khan FS, Bhaskar H. Advances in the quantum theoretical approach to image processing applications. *ACM Comput Surv*. 2017;49(4):1-49.
21. Rieffel E, Polak W. An introduction to quantum computing for non-physicists. *ACM Comput Surv*. 2000;32(3):300-335.
22. Nejatollahi H, Dutt N, Ray S, Regazzoni F, Banerjee I, Cammarota R. Post-quantum lattice-based cryptography implementations: a survey. *ACM Comput Surv*. 2019;51(6):1-41.
23. Devitt SJ, Stephens AM, Munro WJ, Nemoto K. Analysis of an atom-optical architecture for quantum computation. In: Yamamoto Y, Semba K, eds. *Principles and Methods of Quantum Information Technologies*. Springer; 2016:407-437.
24. Bravyi S, Gosset D, König R. Quantum advantage with shallow circuits. *Science*. 2018;362(6412):308-311. <https://doi.org/10.1126/science.aar3106>
25. Bremner MJ, Montanaro A, Shepherd DJ. Achieving quantum supremacy with sparse and noisy commuting quantum computations. *Quantum*. 2017;1:8. <https://doi.org/10.22331/q-2017-04-25-8>
26. Dennis E, Kitaev A, Landahl A, Preskill J. Topological quantum memory. *J Math Phys*. 2002;43(9):4452-4505. <https://doi.org/10.1063/1.1499754>
27. Van Meter RD. *Architecture of a Quantum Multicomputer Optimized for Shor's Factoring Algorithm*. arXiv [quant-ph]; 2006.
28. Van Meter R, Devitt SJ. The path to scalable distributed quantum computing. *Computer*. 2016;49(9):31-42. <https://doi.org/10.1109/mc.2016.291>
29. Nagayama S, Fowler AG, Horsman D, Devitt SJ, Van Meter R. Surface code error correction on a defective lattice. *New J Phys*. 2017;19(2):023050.
30. Hey T. Quantum computing: an introduction. *Comput Control Eng J*. 1999;10(3):105-112. <https://doi.org/10.1049/cce:19990303>
31. Fowler AG, Devitt SJ, Hollenberg LCL. Implementation of Shor's algorithm on a linear nearest neighbour qubit array. *Quantum Inf Comput*. 2004;4(4):237-251.
32. Jain S. Quantum computer architectures: a survey. *Proceedings of the 2015 2nd International Conference on Computing for Sustainable Global Development*; 2015:2165-2169.
33. Buhrman H, Rohrig H. Distributed quantum computing. *Math Found Comput Sci*. 2003;2747:1-20.
34. Zhang GX. Quantum-inspired evolutionary algorithms: a survey and empirical study. *J Heuristics*. 2011;17(3):303-351. <https://doi.org/10.1007/s10732-010-9136-0>
35. Li W, Cao J, Wu J, Huang C, Buyya R. A collaborative filtering recommendation method based on discrete quantum-inspired shuffled frog leaping algorithms in social networks. *Futur Gener Comput Syst*. 2018;88:262-270.
36. Han KH, Kim JH. Quantum-inspired evolutionary algorithm for a class of combinatorial optimization. *IEEE Trans Evol Comput*. 2002;6(6):580-593. <https://doi.org/10.1109/tevc.2002.804320>
37. Rotteler M. Quantum algorithms: a survey of some recent results. *Comput Sci Dev*. 2006;21(1-2):3-20. <https://doi.org/10.1007/s00450-006-0008-7>
38. Li YY, Tian MZ, Liu GY, Peng C, Mao LC. Quantum optimization and quantum learning: a survey. *IEEE Access*. 2020;8:23568-23593. <https://doi.org/10.1109/access.2020.2970105>
39. Sofge DA. A survey of quantum programming languages: history, methods, and tools. *Proceedings of the 2008 2nd International Conference on Quantum, Nano and Micro Technologies (ICQNM)*; 2008:66-71. <https://doi.org/10.1109/icqnm.2008.15>

40. Gay SJ. Quantum programming languages: survey and bibliography. *Math Struct Comput Sci*. 2006;16(4):581-600. <https://doi.org/10.1017/s0960129506005378>
41. Menon PS, Ritwik M. A comprehensive but not complicated survey on quantum computing. *Int Conf Futur Inf Eng*. 2014;10:144-152. <https://doi.org/10.1016/j.ieri.2014.09.069>
42. Kumar K, Sharma NA, Prasad R. A survey on quantum computing with Main focus on the methods of implementation and commercialization gaps. Proceedings of the 2015 2nd Asia-Pacific World Congress on Computer Science and Engineering (APWC on CSE 2015); 2015:1-7.
43. Shaikh TA, Ali R. Quantum computing in big data analytics: a survey. Proceedings of the 2016 IEEE International Conference on Computer and Information Technology; 2016:112-115. <https://doi.org/10.1109/cit.2016.79>
44. Yan F, Iliyasu AM, Venegas-Andraca SE. A survey of quantum image representations. *Quantum Inf Process*. 2016;15(1):1-35. <https://doi.org/10.1007/s11128-015-1195-6>
45. Roetteler M, Svore KM. Quantum computing: codebreaking and beyond. *IEEE Secur Priv*. 2018;16(5):22-36. <https://doi.org/10.1109/msp.2018.3761710>
46. Deutsch D, Jozsa R. Rapid solution of problems by quantum computation. *Proc Royal Soc Lond Ser A Math Phys Sci*. 1992;439(1907):553-558.
47. Bernstein E, Vazirani U. Quantum complexity theory. *SIAM J Comput*. 1997;26(5):1411-1473. <https://doi.org/10.1137/S0097539796300921>
48. Simon DR. On the power of quantum computation. *SIAM J Comput*. 1997;26(5):1474-1483.
49. Shor PW. Algorithms for quantum computation: discrete logarithms and factoring. Proceedings 35th Annual Symposium on Foundations of Computer Science; 1994:124-134; IEEE.
50. Grover LK. A fast quantum mechanical algorithm for database search. Proceedings of the 28th Annual ACM Symposium on Theory of Computing; 1996:212-219; ACM.
51. Gilles PH, Tapp A. Quantum counting. Proceedings of the International Colloquium on Automata, Languages, and Programming; 1998:820-831; Springer.
52. Farhi E, Goldstone J, Gutmann S. A quantum approximate optimization algorithm; 2014. arXiv:1411.4028.
53. Qiang XG, Zhou XQ, Wang JW, et al. Large-scale silicon quantum photonics implementing arbitrary two-qubit processing. *Nat Photonics*. 2018;12(9):534-539. <https://doi.org/10.1038/s41566-018-0236-y>
54. Bernstein DJ, Lange T. Post-quantum cryptography. *Nature*. 2017;549(7671):188-194.
55. Bernstein DJ, Heninger N, Lou P, Valenta L. Post-Quantum RSA. Proceedings of the International Workshop on Post-Quantum Cryptography; 2017:311-329; Springer.
56. Bernstein DJ. Introduction to post-quantum cryptography. In: Bernstein DJ, Buchmann J, Dahmen E, eds. *Post-Quantum Cryptography*. Springer; 2009:1-14.
57. The QX Simulator. <http://quantum-studio.net/>
58. Freivalds R. How to simulate free will in a computational device. *ACM Comput Surv*. 1999;31(3es):15-es.
59. Weitenberg C, Kuhr S, Molmer K, Sherson JF. Quantum computation architecture using optical tweezers. *Phys Rev A*. 2011;84(3):032322. <https://doi.org/10.1103/PhysRevA.84.032322>
60. Tomza M, Jachymski K, Gerritsma R, et al. Cold hybrid ion-atom systems. *Rev Mod Phys*. 2019;91(3):035001. <https://doi.org/10.1103/RevModPhys.91.035001>
61. O'Gorman J, Nickerson NH, Ross P, Morton JLL, Benjamin SC. A silicon-based surface code quantum computer. *npj Quantum Inf*. 2016;2:15019. <https://doi.org/10.1038/npjqi.2015.19>
62. Compagno E, Banchi L, Bose S. Toolbox for linear optics in a one-dimensional lattice via minimal control. *Phys Rev A*. 2015;92(2):022701. <https://doi.org/10.1103/PhysRevA.92.022701>
63. Schaal S, Barraud S, Morton JLL, Gonzalez-Zalba MF. Conditional dispersive readout of a CMOS single-electron memory cell. *Phys Rev Appl*. 2018;9(5):054016. <https://doi.org/10.1103/PhysRevApplied.9.054016>
64. Zwanenburg FA, Dzurak AS, Morello A, et al. Silicon quantum electronics. *Rev Mod Phys*. 2013;85(3):961. <https://doi.org/10.1103/RevModPhys.85.961>
65. Veldhorst M, Yang CH, Hwang JCC, et al. A two-qubit logic gate in silicon. *Nature*. 2015;526(7573):410-414. <https://doi.org/10.1038/nature15263>
66. Mizuta R, Otxoa RM, Betz AC, Gonzalez-Zalba MF. Quantum and tunneling capacitance in charge and spin qubits. *Phys Rev B*. 2017;95(4):045414. <https://doi.org/10.1103/PhysRevB.95.045414>
67. de Albornoz ACC, Taylor J, Carare V. Time-optimal implementations of quantum algorithms. *Phys Rev A*. 2019;100(3):032329. <https://doi.org/10.1103/PhysRevA.100.032329>
68. Jones T, Brown A, Bush I, Benjamin SC. Quest and high performance simulation of quantum computers. *Sci Rep*. 2019;9(1):1-11.
69. Amy M, Gheorghiu V. staq—a full-stack quantum processing toolkit. *Quantum Sci Technol*. 2020;5:034016.
70. JavadiAbhari A, Patil S, Kudrow D, et al. ScaffCC: scalable compilation and analysis of quantum programs. *Parallel Comput*. 2015;45:2-17.
71. Naeem W, Chuhdhry Y. *Q-Studio*. Doctoral dissertation. Department of Computer Science, COMSATS University Islamabad, Lahore Campus; 2019.
72. Gheorghiu V. Quantum++—a C++ 11 quantum computing library; 2014. arXiv:1412.4704.
73. Miller DM, Thornton MA. QMDD: a decision diagram structure for reversible and quantum circuits. Proceedings of the 36th International Symposium on Multiple-Valued Logic (ISMVL'06); 2006:30; IEEE.

74. Aaronson S, Toth B. Simulation and synthesis of stabilizer quantum circuits; 2003.
75. Brandhorst-Satzkorn J. A review of freely available quantum computer simulation software; 2012.
76. Mlnarik H. *Quantum Programming Language LanQ*. Faculty of Informatics, Masaryk University; 2007.
77. Glendinning I, Ömer B. Parallelization of the QC-lib quantum computer simulator library. *Proceedings of the International Conference on Parallel Processing and Applied Mathematics*; 2003:461-468; Springer.
78. da Silva Feitosa S, da Silva Bueno JA. Simulating quantum parallelism in CPU and GPU using the LibQuantum library. *ComInG-Commun Innov Gazette Mag*. 2016;1(2):26-36.
79. Schneider SSD. *Quantum Systems Simulator*. Doctoral dissertation. Massachusetts Institute of Technology; 2000.
80. Ivancova O, Korenkov V, Tyatyushkina O, Ulyanov S, Fukuda T. Quantum supremacy in end-to-end intelligent IT. Pt. I: quantum software engineering-quantum gate level applied models simulators. *Syst Anal Sci Educ*. 2020;2020(1):52-84.
81. Qubit Workbench. <https://elyah.io/product>
82. Linear AI. <http://linearai.sourceforge.net/>
83. Nielsen E, Gao X, Kalashnikova I, Muller RP, Salinger AG, Young RW. QCAD simulation and optimization of semiconductor double quantum dots. Technical report. Sandia National Laboratories; 2013.
84. Beals TR. *Quantum Communication and Information Processing*. University of California; 2008.
85. Caraiman S, Archip A, Manta V. A grid enabled quantum computer simulator. *Proceedings of the 2009 11th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing*; 2009:189-196; IEEE.
86. QOCS. <https://github.com/dillanchang/QOCS>
87. Q++. <https://sourceforge.net/projects/qplusplus/>
88. Moran CC. Quintuple: a python 5-qubit quantum computer simulator to facilitate cloud quantum computing; 2016. arXiv:1606.09225.
89. Dekant H. Artiste-qb-net/quantum-fog: python tools for analyzing both classical 29 and quantum Bayesian Networks [Electronic resource]/Dekant Henning, Tregillus Henry, Tucci Robert, Yin Tao; 2019. <https://github.com/artiste-qb-net/quantum-fog>
90. Patrzyk J, Patrzyk B, Rycerz K, Bubak M. Towards a novel environment for simulation of quantum computing. *Comput Sci*. 2015;16(1):103-129.
91. Tankasala A, Ilatikhameneh H. Quantum-kit: simulating Shor's factorization of 24-bit number on desktop; 2019. arXiv:1908.07187.
92. Huo C. *A Bloch Sphere Animation Software Using a Three Dimensional Java Simulator*. Doctoral dissertation. University of Cincinnati; 2009.
93. BackupBrain. <https://backupbrain.github.io/quantum-compiler-simulator/>
94. Viamontes GF, Markov IL, Hayes JP. *Quantum Circuit Simulation*. Springer Science & Business Media; 2009.
95. Srivastava R, Choi I, Cook T, NUE Team. *The Commercial Prospects for Quantum Computing*. Networked Quantum Information Technologies; 2016.
96. Glos A, Miszczak JA, Ostaszewski M. QSWalk. JI: Julia package for quantum stochastic walks analysis. *Comput Phys Commun*. 2019;235:414-421.
97. Krämer S, Plankensteiner D, Ostermann L, Ritsch H. QuantumOptics. JI: a Julia framework for simulating open quantum systems. *Comput Phys Commun*. 2018;227:109-116.
98. QuantumWalk.jl. <https://github.com/iitis/QuantumWalk.jl>
99. Radtke T, Fritzsche S. Simulation of n-qubit quantum systems. I quantum registers and quantum gates. *Comput Phys Commun*. 2005;173(1-2):91-113.
100. McCubbin CB. *Openquacs, an Open-Source Quantum Computation Simulator in Maple*. Doctoral dissertation. University of Maryland, Baltimore County; 2000.
101. Feito A. Quantavo: a maple toolbox for linear quantum optics; 2008. arXiv:0806.2171.
102. Juliá-Díaz B, Burdis JM, Tabakin F. QDENSITY—a Mathematica quantum computer simulation. *Comput Phys Commun*. 2006;174(11):914-934.
103. Quantum. <http://homepage.cem.itesm.mx/igomez/quantum/index.htm>
104. Hincks IN, Granade CE, Borneman TW, Cory DG. Controlling quantum devices with nonlinear hardware. *Phys Rev Appl*. 2015;4(2):024012.
105. Qi. <https://github.com/iitis/qi>
106. Tolba AS, Rashad MZ, El-Dosuky MA. Q#, a quantum computation package for the .NET platform; 2013. arXiv:1302.5133.
107. Terörde M. Registry-spuren verursacht durch die quantenprogrammiersprache Q; 2019.
108. Drqubit. <http://www.dr-qubit.org/matlab.php>
109. Tóth G. QUBIT4MATLAB V3. 0: a program package for quantum information science and quantum optics for MATLAB. *Comput Phys Commun*. 2008;179(6):430-437.
110. Patrzyk J. *Graphical and Programming Support for Simulations of Quantum Computations*. Master of Science thesis. Supervised by Katarzyna Rycerz; 2014.
111. Quantum.NET. <https://github.com/phbaudin/quantum-computing>
112. Omole V, Tyagi A, Carey C, et al. Cirq: a python framework for creating, editing, and invoking quantum circuits; 2019. <https://github.com/quantumlib/Cirq>
113. Steiger DS, Häner T, Troyer M. ProjectQ: an open source software framework for quantum computing. *Quantum*. 2018;2:49.
114. Zagorodko PV. *Research of Possibilities of Quantum Programming for Realization of Tasks of Machine Learning*. Doctoral dissertation; 2020.

115. Cross A. The IBM Q experience and QISKit open-source quantum computing software. *APS*. 2018;2018:L58-003.
116. McKay DC, Alexander T, Bello L, et al. Qiskit backend specifications for OpenQASM and OpenPulse experiments; 2018. arXiv:1809.03452.
117. Kelly A. Simulating quantum computers using OpenCL; 2018. arXiv:1805.00988.
118. Altenkirch T, Green AS. The quantum IO monad. In: Simon G, Ian M, eds. *Semantic Techniques in Quantum Computation*; Cambridge University Press; 2010:173-205.
119. Qchas. <https://hackage.haskell.org/package/qchas>
120. Quantum User Interface. <https://qui.research.unimelb.edu.au/>
121. Quantum Development Kit (QDK) for azure quantum; 2021. <https://www.microsoft.com/en-us/quantum/development-kit>
122. Zhao J. Quantum software engineering: landscapes and horizons; 2020. arXiv preprint arXiv:2007.07047.
123. Piattini M, Serrano M, Perez-Castillo R, Petersen G, Hevia JL. Toward a quantum software engineering. *IT Prof.* 2021;23(1):62-66.
124. Miranskyy A, Zhang L, Doliskani J. On testing and debugging quantum software; 2021. arXiv preprint arXiv:2103.09172.
125. Selinger P. A brief survey of quantum programming languages. *Proceedings of the International Symposium on Functional and Logic Programming*; 2004:1-6; Springer.
126. Heim B, Soeken M, Marshall S, et al. Quantum programming languages. *Nat Rev Phys.* 2020;2(12):709-722.
127. Staton S. Algebraic effects, linearity, and quantum programming languages. *ACM SIGPLAN Not.* 2015;50(1):395-406.
128. Mischczak JA. Models of quantum computation and quantum programming languages; 2010. arXiv preprint arXiv:1012.6035.
129. Unruh D. Quantum programming languages. *Informatik-Forschung Und Entwicklung.* 2006;21(1-2):55-63.
130. Fu P, Kishida K, Selinger P. Linear dependent type theory for quantum programming languages. *Proceedings of the 35th Annual ACM/IEEE Symposium on Logic in Computer Science*; 2020:440-453.
131. Chong FT, Franklin D, Martonosi M. Programming languages and compiler design for realistic quantum hardware. *Nature.* 2017;549(7671):180-187.
132. Oskin M, Chong FT, Chuang IL. A practical architecture for reliable quantum computers. *Computer.* 2002;35(1):79-87.
133. Metodi TS, Thaker DD, Cross AW, Chong FT, Chuang IL. A quantum logic array microarchitecture: scalable quantum data movement and computation. *Proceedings of the 38th Annual IEEE/ACM International Symposium on Microarchitecture (MICRO'05)*; 2005:12-pp; IEEE.
134. Riesebois L, Bondurant B, Brown KR. Universal graph-based scheduling for quantum systems. *IEEE Micro.* 2021;41:57-65.
135. Saad HM, Chakraborty RK, Elsayed S, Ryan MJ. Quantum-inspired genetic algorithm for resource-constrained project-scheduling. *IEEE Access.* 2021;9:38488-38502.
136. Kong W, Wang J, Han Y, et al. Origin pilot: a quantum operating system for efficient usage of quantum resources; 2021. arXiv preprint arXiv:2105.10730.
137. Bassoli R, Boche H, Deppe C, et al. Quantum communication networks: design and simulation. In: Bassoli R, Boche H, Deppe C, Ferrara R, Fitzek FHP, Janssen G, Saeedinaeeni S, eds. *Quantum Communication Networks*. Springer; 2021:187-209.
138. Mohammadzadeh N, Zamani MS, Sedighi M. Quantum circuit physical design methodology with emphasis on physical synthesis. *Quantum Inf Process.* 2014;13(2):445-465.
139. Mirkhani Z, Mohammadzadeh N. Physical synthesis of quantum circuits using templates. *Quantum Inf Process.* 2016;15(10):4117-4135.
140. Mohammadzadeh N, Sedighi M, Zamani MS. Quantum physical synthesis: improving physical design by netlist modifications. *Microelectron J.* 2010;41(4):219-230.
141. Krüger T, Mauere W. Quantum annealing-based software components: an experimental case study with sat solving. *Proceedings of the IEEE/ACM 42nd International Conference on Software Engineering Workshops*; 2020:445-450.
142. Nath RK, Thapliyal H, Humble TS. Quantum annealing for automated feature selection in stress detection; 2021. arXiv preprint arXiv:2106.05134.
143. Ayanzadeh R, Dorband JE, Halem M, Finin T. Multi-qubit correction for quantum annealers. *Nat Sci Rep.* 2021;11:16119.
144. Ayanzadeh R, Halem M, Finin T. Reinforcement quantum annealing: a hybrid quantum learning automata. *Sci Rep.* 2020;10(1):1-11.
145. Dixit V, Selvarajan R, Aldwairi T, et al. Training a quantum annealing based restricted boltzmann machine on cybersecurity data. *IEEE Trans Emerg Top Comput Intell.* 2021.
146. Krauss T, McCollum J, Pendery C, Litwin S, Michaels AJ. Solving the max-flow problem on a quantum annealing computer. *IEEE Trans Quantum Eng.* 2020;1:1-10.
147. Piattini M, Petersen G, Pérez-Castillo R, et al. The Talavera manifesto for quantum software engineering and programming. *QANSWER*; TNO Publications; 2020:1-5.
148. Weder B, Barzen J, Leymann F, Salm M, Vietz D. The quantum software lifecycle. *Proceedings of the 1st ACM SIGSOFT International Workshop on Architectures and Paradigms for Engineering Quantum Software*; 2020:2-9.
149. Mastriani M, Iyengar SS, Kumar L. Satellite quantum communication protocol regardless of the weather. *Opt Quant Electron.* 2021;53(4):1-14.
150. Conrad A, Hill A, Chaffee D, et al. Drone-based quantum key distribution. *Proceedings of the APS Division of Atomic, Molecular and Optical Physics Meeting Abstracts*; Vol. 2019, 2019:08-003.
151. Kumar A, Sharma K, Singh H, Naugriya SG, Gill SS, Buyya R. A drone-based networked system and methods for combating coronavirus disease (COVID-19) pandemic. *Futur Gener Comput Syst.* 2021;115:1-19.
152. Singh H, Tyagi S, Kumar P, Gill SS, Buyya R. Metaheuristics for scheduling of heterogeneous tasks in cloud computing environments: analysis, performance evaluation, and future directions. *Simul Model Pract Theory.* 2021;102353.

153. Kumar A, Bhatia S, Kaushik K, et al. Survey of promising technologies for quantum drones and networks. *IEEE Access*. 2021;9:125868-125911. <https://doi.org/10.1109/ACCESS.2021.3109816>
154. Tsai CW, Yang CW, Lin J, Chang YC, Chang RS. Quantum key distribution networks: challenges and future research issues in security. *Appl Sci*. 2021;11(9):3767.
155. Qassim Y, Magaña ME, Yavuz A. Post-quantum hybrid security mechanism for MIMO systems. Proceedings of the 2017 International Conference on Computing, Networking and Communications (ICNC); 2016:84-689.
156. Deutsch D, Ekert A, Jozsa R, Macchiavello C, Popescu S, Sanpera A. Quantum privacy amplification and the security of quantum cryptography over noisy channels. *Phys Rev Lett*. 1996;77(13):2818-2821.
157. Naik DS, Peterson CG, White AG, Berglund AJ, Kwiat PG. Entangled state quantum cryptography: eavesdropping on the Ekert protocol. *Phys Rev Lett*. 2000;84(20):4733-4736.
158. Elbouchari M, Azizi M, Azizi A. Quantum key distribution protocols: a survey. *Int J Univ Comput Sci*. 2010;1(2):59-67.
159. Bugge AN, Sauge S, Ghazali AMM, Skaar J, Lydersen L, Makarov V. Laser damage helps the eavesdropper in quantum cryptography. *Phys Rev Lett*. 2014;112(7):070503.
160. Jain N, Anisimova E, Khan I, Makarov V, Marquardt C, Leuchs G. Trojan-horse attacks threaten the security of practical quantum cryptography. *New J Phys*. 2014;16(12):123030.
161. Li J, Li N, Zhang Y, et al. A survey on quantum cryptography. *Chin J Electron*. 2018;27(2):223-228.
162. Bennett CH, Brassard G. Quantum cryptography: public key distribution and coin tossing; 2020. arXiv:2003.06557.
163. Bhusal N, Lohani S, You C, et al. Spatial mode correction of single photons using machine learning; 2020. arXiv:2006.07760.
164. Brassard G, Lütkenhaus N, Mor T, Sanders BC. Limitations on practical quantum cryptography. *Phys Rev Lett*. 2000;85(6):1330-1333.
165. Durak K, Jam N. An attack to quantum systems through RF radiation tracking; 2020. arXiv:2004.14445.
166. Gras G, Sultana N, Huang A, et al. Optical control of single-photon negative-feedback avalanche diode detector. *J Appl Phys*. 2020;127(9):094502.
167. Guo PL, Dong C, He Y, et al. Efficient quantum key distribution against collective noise using polarization and transverse spatial mode of photons. *Opt Express*. 2020;28(4):4611-4624.
168. Huang A, Li R, Egorov V, Tchouragoulov S, Kumar K, Makarov V. Laser-damage attack against optical attenuators in quantum key distribution. *Phys Rev Appl*. 2020;13(3):034017.
169. Melhem M, Chamon C, Ferdous S, Kish LB. AC loop current attacks against the KLJN secure key exchange scheme; 2020. arXiv:2005.11002.
170. Qi B, Evans PG, Grice WP, UT-Battelle LLC. Quantum key distribution using a thermal source; 2020. U.S. patent application 16/197,457.
171. Shang T, Tang Y, Chen R, Liu J. Full quantum one-way function for quantum cryptography. *Quantum Eng*. 2020;2(1):e32.
172. Trushechkin A. Security of quantum key distribution with detection-efficiency mismatch in the multiphoton case; 2020. arXiv:2004.07809.
173. Vybornyi I, Trichili A, Alouini MS. Backflash light as a security vulnerability in quantum key distribution systems; 2020. arXiv:2003.10478.
174. Yin J, Li YH, Liao SK, et al. Entanglement-based secure quantum cryptography over 1,120 kilometres. *Nature*. 2020;582(7813):501-505.
175. Zhang Y, Coles PJ, Winick A, Lin J, Lutkenhaus N. Security proof of practical quantum key distribution with detection-efficiency mismatch; 2020. arXiv:2004.04383.
176. Zhou Y, Braverman B, Fyffe A, Zhang R, Zhao J, Willner AE, Shi Z, Boyd RW. High-fidelity spatial mode transmission through multimode fiber via vectorial time reversal; 2020. arXiv:2003.09883.
177. Ekert AK. Quantum cryptography based on Bell's theorem. *Phys Rev Lett*. 1991;67(6):661-663.
178. Ghalaii M, Ottaviani C, Kumar R, Pirandola S, Razavi M. Discrete-modulation continuous-variable quantum key distribution enhanced by quantum scissors. *IEEE J Select Areas Commun*. 2020;38(3):506-516.
179. Nemoto K, Devitt S, Munro WJ. Noise management to achieve superiority in quantum information systems. *Philos Trans R Soc A Math Phys Eng Sci*. 2017;375(2099):20160236.
180. Bennett CH. Quantum cryptography using any two nonorthogonal states. *Phys Rev Lett*. 1992;68(21):3121-3124.
181. Bennett CH, Brassard G, Ekert AK. Quantum cryptography. *Sci Am*. 1992;267(4):50-57.
182. Li J, Guo Y, Wang X, Xie C, Zhang L, Huang D. Discrete-modulated continuous-variable quantum key distribution with a machine-learning-based detector. *Opt Eng*. 2018;57(6):066109.
183. Hatakeyama Y, Mizutani A, Kato G, Imoto N, Tamaki K. Differential-phase-shift quantum-key-distribution protocol with a small number of random delays. *Phys Rev A*. 2017;95(4):042301.
184. Schrenk B, Hentschel M, Hübel H. Single-laser differential phase shift transmitter for small form-factor quantum key distribution optics. Proceedings of the 2018 Optical Fiber Communications Conference and Exposition (OFC); 1-3; IEEE.
185. Valivarthi R, Etcheverry S, Aldama J, Zwiehoff F, Pruneri V. Plug-and-play continuous-variable quantum key distribution for metropolitan networks. *Opt Express*. 2020;28(10):14547-14559.
186. Leverrier A, Grangier P. Unconditional security proof of long-distance continuous-variable quantum key distribution with discrete modulation. *Phys Rev Lett*. 2009;102(18):180504.
187. Lin J, Upadhyaya T, Lütkenhaus N. Asymptotic security analysis of discrete-modulated continuous-variable quantum key distribution. *Phys Rev X*. 2019;9(4):041064.
188. Ruan X, Zhang H, Zhao W, Wang X, Li X, Guo Y. Security analysis of discrete-modulated continuous-variable quantum key distribution over seawater channel. *Appl Sci*. 2019;9(22):4956.

189. Stucki D, Fasel S, Gisin N, Thoma Y, Zbinden H. Coherent one-way quantum key distribution. In: Miloslav D, Mark SH, Wolfgang PS, Ivan P, Alan LM, Alexandre P, eds. *Photon Counting Applications, Quantum Optics, and Quantum Cryptography*. Vol 6583. International Society for Optics and Photonics; 2007:65830L.
190. Mafu M, Senekane M. *Security in Quantum Key Distribution Protocols*. IntechOpen; 2018.
191. Mafu M, Marais A, Petruccione F. A necessary condition for the security of coherent-one-way quantum key distribution protocol. *Appl Math Inf Sci*. 2014;8(6):2769-2773.
192. Mafu M, Marais A, Petruccione F. Towards the unconditional security proof for the coherent-one-way protocol. 2011.
193. Wonfor A, White C, Bahrami A, et al. Field trial of multi-node, coherent-one-way quantum key distribution with encrypted 5×100G DWDM transmission system. Proceedings of the 45th European Conference on Optical Communication (ECOC 2019); 2019:1-4; IET.
194. Alhussein M, Inoue K. Differential phase shift quantum key distribution with variable loss revealing blinding and control side-channel attacks. *Jpn J Appl Phys*. 2019;58(10):102001.
195. Collins RJ, Amir R, Fujiwara M, et al. Experimental transmission of quantum digital signatures over 90 km of installed optical fiber using a differential phase shift quantum key distribution system. *Opt Lett*. 2016;41(21):4883-4886.
196. Sibson P, Erven C, Godfrey M, et al. Chip-based quantum key distribution. *Nat Commun*. 2017;8(1):1-6.
197. Lo HK. Proof of unconditional security of six-state quantum key distribution scheme; 2001. arXiv quant-ph/0102138.
198. Azuma H, Ban M. The intercept/resend attack and the collective attack on the six-state protocol of the quantum key distribution; 2019. arXiv:1912.00196.
199. Chau HF, Yin ZQ, Wang S, Chen W, Han ZF. Chau–Wang–Wong17 scheme is experimentally more feasible than the six-state scheme. *Quantum Inf Process*. 2019;18(5):138.
200. Liu H, Yu ZW, Zou M, et al. Experimental 4-intensity decoy-state quantum key distribution with asymmetric basis-detector efficiency. *Phys Rev A*. 2019;100(4):042313.
201. Grasselli F, Curty M. Practical decoy-state method for twin-field quantum key distribution. *New J Phys*. 2019;21(7):073001.
202. Chau HF, Ng KJ. Application of an improved version of McDiarmid inequality in finite-key-length decoy-state quantum key distribution. *New J Phys*. 2020;22(2):023011.
203. Liu F, Zhou C, Wang Y, Gan Y, Jiang M, Bao W. Improved secure bounds for passive decoy state quantum key distribution system. *Opt Quant Electron*. 2020;52(3):1-15.
204. Kozziel B, Azarderakhsh R, Kermani MM, Jao D. Post-quantum cryptography on FPGA based on isogenies on elliptic curves. *IEEE Trans Circuits Syst I Regul Pap*. 2016;64(1):86-99.
205. Ding J, Yang BY. Post-quantum cryptography. In: Ding J, Petzoldt A, Schmidt DS, eds. *Multivariate Public-Key Cryptography*. Springer; 2009:193-241.
206. Shrestha SR, Kim YS. New McEliece cryptosystem based on polar codes as a candidate for post-quantum cryptography. Proceedings of the 2014 14th International Symposium on Communications and Information Technologies (ISCIT); 2014:368-372; IEEE.
207. Ajtai M. Generating hard instances of lattice problems. Proceedings of the 28th Annual ACM Symposium on Theory of Computing; 1996:99-108.
208. Regev O. On lattices, learning with errors, random linear codes, and cryptography. *J ACM*. 2009;56(6):1-40.
209. Akleyek S, Seyhan K. A probably secure bi-GISIS based modified AKE scheme with reusable keys. *IEEE Access*. 2020;8:26210-26222.
210. El Kassem N. *Lattice-Based Direct Anonymous Attestation*. Doctoral dissertation. University of Surrey; 2020.
211. Xu Z, He D, Vijayakumar P, Choo KKR, Li L. Efficient NTRU lattice-based Certificateless signature scheme for medical cyber-physical systems. *J Med Syst*. 2020;44(5):1-8.
212. Langlois A, Stehlé D. Worst-case to average-case reductions for module lattices. *Des Codes Crypt*. 2015;75(3):565-599.
213. Plantard T, Schneider M. Creating a challenge for ideal lattices. *IACR Cryptol ePrint Arch*. 2013;2013:39.
214. Lyubashevsky V, Nguyen NK, Seiler G. SMILE: set membership from ideal lattices with applications to ring signatures and confidential transactions. In: Malkin T, Peikert C, eds. *CRYPTO*; Springer International Publishing; 2021:611-640.
215. Bai S, Das D, Hiromasa R. MPSign: a signature from Small-secret middle-product learning with errors. Proceedings of the IACR International Conference on Public-Key Cryptography; 2020:66-93; Springer.
216. Banerjee U, Ukyab TS, Chandrakasan AP. Sapphire: a configurable crypto-processor for post-quantum lattice-based protocols; 2019. arXiv:1910.07557.
217. Mera JMB, Turan F, Karmakar A, Roy SS, Verbaudhede I. Compact domain-specific co-processor for accelerating module lattice-based key encapsulation mechanism. *IACR Cryptol ePrint Arch*. 2020;2020:321.
218. Nejatollahi H, Valencia F, Banik S, Regazzoni F, Cammarota R, Dutt N. Synthesis of flexible accelerators for early adoption of ring-lwe post-quantum cryptography. *ACM Trans Embedded Comput Syst*. 2020;19(2):1-17.
219. McEliece RJ. A public-key cryptosystem based on algebraic. *Coding Thv*. 1978;4244:114-116.
220. Jäämeri E. *Code-based Cryptography*. Master's thesis. Aalto University, Finland; 2020. Accessed April 22, 2021. https://aaltodoc.aalto.fi/bitstream/handle/123456789/42736/master_J%C3%A4%C3%A4meri_Elias_2020.pdf?sequence=1
221. Singh H. Code based cryptography: classic McEliece; 2019. arXiv:1907.12754
222. Bardet M, Briaud P, Bros M, et al. An algebraic attack on rank metric code-based cryptosystems. Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques; 2020:64-93; Springer.
223. Ezerman MF, Lee HT, Ling S, Nguyen K, Wang H. Provably secure group signature schemes from code-based assumptions. *IEEE Trans Inf Theory*. 2020;66:5754-5773.

224. Fernández-Caramés TM. From pre-quantum to post-quantum IoT security: a survey on quantum-resistant cryptosystems for the Internet of Things. *IEEE Internet Things J.* 2019;7(7):6457-6480.
225. Chang C, Srirama SN, Buyya R. Mobile cloud business process management system for the internet of things: a survey. *ACM Comput Surv.* 2016;49(4):1-42.
226. Cayrel PL, Colombier B, Drăgoi VF, Menu A, Bossuet L. Message-recovery laser fault injection attack on the classic McEliece cryptosystem. *Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques*; 2021:438-467; Springer.
227. Cohen A, D'Oliveira RG, Salamatian S, Médard M. Network coding-based post-quantum cryptography. *IEEE J Select Areas Inf Theory.* 2021;2(1):49-64.
228. Doron D, Moshkovitz D, Oh J, Zuckerman D. Nearly optimal pseudorandomness from hardness. *Proceedings of the 2020 IEEE 61st Annual Symposium on Foundations of Computer Science (FOCS)*; 2020:1057-1068; IEEE.
229. Couvreur A, Debris-Alazard T, Gaborit P. On the hardness of code equivalence problems in rank metric; 2020. arXiv preprint arXiv:2011.04611.
230. Singh S, Chana I, Singh M. The journey of QoS-aware autonomic cloud computing. *IT Prof.* 2017;19(2):42-49.
231. Alagic G, Alagic G, Alperin-Sheriff J, et al. *Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process*. US Department of Commerce, National Institute of Standards and Technology; 2019.
232. Cartor, R. *A Study of Big Field Multivariate Cryptography*, University of Louisville; 2019.
233. Smith-Tone D, Tone C. A nonlinear multivariate cryptosystem based on a random linear code. *IACR Cryptol ePrint Arch.* 2019;2019:1355.
234. Shen R, Xiang H, Zhang X, Cai B, Xiang T. Application and implementation of multivariate public key cryptosystem in blockchain (short paper). *Proceedings of the International Conference on Collaborative Computing: Networking, Applications and Worksharing*; 2019:419-428; Springer.
235. Silva Pinheiro Bittencourt M Reducing keys in rainbow-like signature schemes; 2019.
236. Štumpf D. Cryptoanalysis of a post-quantum cryptography algorithm; 2020.
237. Matsumoto T, Imai H. Public quadratic polynomial-tuples for efficient signature-verification and message-encryption. In: Barstow D, Brauer W, Hansen PB, et al., eds. *Advances in Cryptology—EUROCRYPT '88*. Springer; 1988:419-453.
238. Peng C, Chen J, Zeadally S, He D. Isogeny-based cryptography: a promising post-quantum technique. *IT Prof.* 2019;21(6):27-32.
239. Petit C, Lauter KE. Hard and easy problems for Supersingular isogeny graphs. *IACR Cryptol ePrint Arch.* 2017;2017:962.
240. Galbraith SD, Petit C, Shani B, Ti YB. On the security of supersingular isogeny cryptosystems. *Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security*; 2016:63-91; Springer.
241. Beullens W, Kleinjung T, Vercauteren F. CSI-FiSh: efficient isogeny based signatures through class group computations. *Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security*; 2019:227-247; Springer.
242. Srinath MS, Chandrasekaran V. Isogeny-based quantum-resistant undeniable blind signature scheme. *IACR Cryptol ePrint Arch.* 2016;2016:148.
243. Sahu RA, Gini A, Pal A. Supersingular isogeny-based designated verifier blind signature. *IACR Cryptol ePrint Arch.* 2019;2019:1498.
244. Doliskani J, Pereira GC, Barreto PS. Faster cryptographic hash function from supersingular isogeny graphs. *IACR Cryptol ePrint Arch.* 2017;2017:1202.
245. Castryck W, Decru T, Smith B. Hash functions from superspecial genus-2 curves using Richelot isogenies; 2019. arXiv:1903.06451.
246. Crockett E, Paquin C, Stebila D. Prototyping post-quantum and hybrid key exchange and authentication in TLS and SSH. *IACR Cryptol ePrint Arch.* 2019;2019:858.
247. Campagna M, Crockett E. Hybrid post-quantum key encapsulation methods (PQ KEM) for transport layer security 1.2 (TLS); 2019. Internet Engineering Task Force, Internet-Draft Draft-Campagna-Tls-Bike-Sike-Hybrid-01.
248. Usman M. In-plane polarization anisotropy of ground state optical intensity in InAs/GaAs quantum dots. *J Appl Phys.* 2011;110(9):094512.
249. Ivády V, Davidsson J, Deegan N, et al. Stabilization of point-defect spin qubits by quantum wells. *Nat Commun.* 2019;10(1):1-8.
250. Bertoni A, Bordone P, Brunetti R, Jacoboni C, Reggiani S. Quantum logic gates based on coherent electron transport in quantum wires. *Phys Rev Lett.* 2000;84(25):5912-5915.
251. Vandersypen LM, Steffen M, Breyta G, Yannoni CS, Sherwood MH, Chuang IL. Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance. *Nature.* 2001;414(6866):883-887.
252. Kane BE. A silicon-based nuclear spin quantum computer. *Nature.* 1998;393(6681):133-137.
253. Leuenberger MN, Loss D. Quantum computing in molecular magnets. *Nature.* 2001;410(6830):789-793.
254. Walther H, Varcoe BT, Englert BG, Becker T. Cavity quantum electrodynamics. *Rep Prog Phys.* 2006;69(5):1325-1382.
255. Knill E, Laflamme R, Milburn GJ. A scheme for efficient quantum computation with linear optics. *Nature.* 2001;409(6816):46-52.
256. Neumann P, Mizuochi N, Rempp F, et al. Multipartite entanglement among single spins in diamond. *Science.* 2008;320(5881):1326-1329.
257. Anderlini M, Lee PJ, Brown BL, Sebby-Strabley J, Phillips WD, Porto JV. Controlled exchange interaction between pairs of neutral atoms in an optical lattice. *Nature.* 2007;448(7152):452-456.
258. Longdell JJ, Sellars MJ, Manson NB. Demonstration of conditional quantum phase shift between ions in a solid. *Phys Rev Lett.* 2004;93(13):130503.
259. Náfrádi B, Choucair M, Dinse KP, Forró L. Room temperature manipulation of long lifetime spins in metallic-like carbon nanospheres. *Nat Commun.* 2016;7(1):1-8.
260. Mukai H, Sakata K, Simon D, Wang R, Nakajima Y, Tsai J-S. Packaging large-scale superconducting quantum computer with Airbridge. *APS.* 2019;2019:P26-015.

261. Quantum computing on “Quantum Supremacy” 2020. Accessed August 30, 2020. <https://www.ibm.com/blogs/research/2019/10/on-quantum-supremacy/>
262. Bernhardt C. *Quantum Computing for Everyone*. MIT Press; 2019.
263. Devitt SJ. Performing quantum computing experiments in the cloud. *Phys Rev A*. 2016;94(3):032329.
264. Jurcevic P, Javadi-Abhari A, Bishop LS, et al. Demonstration of quantum volume 64 on a superconducting quantum computing system. *Quantum Sci Technol*. 2021;6(2):025020.
265. Friis N, Marty O, Maier C, et al. Observation of entangled states of a fully controlled 20-qubit system. *Phys Rev X*. 2018;8(2):021012.
266. Kelly J, Barends R, Fowler AG, et al. State preservation by repetitive error detection in a superconducting quantum circuit. *Nature*. 2015;519(7541):66-69.
267. Maurand R, Jehl X, Kotekar-Patil D, et al. A CMOS silicon spin qubit. *Nat Commun*. 2016;7(1):1-6.
268. Hayes AJF, Gilchrist A, Myers CR, Ralph TC. Utilizing encoding in scalable linear optics quantum computing. *J Opt B Quantum Semiclass Opt*. 2004;6(12):533-541.
269. Willett RL, Nayak C, Shtengel K, Pfeiffer LN, West KW. Magnetic-field-tuned aharonov-bohm oscillations and evidence for non-abelian anyons at $\nu = 5/2$. *Phys Rev Lett*. 2013;111(18):186401.
270. Usman M, Ryu H, Woo I, Ebert DS, Klimeck G. Moving toward nano-TCAD through multimillion-atom quantum-dot simulations matching experimental data. *IEEE Trans Nanotechnol*. 2009;8(3):330-344.
271. Hill CD, Peretz E, Hile SJ, et al. A surface code quantum computer in silicon. *Sci Adv*. 2015;1(9):e1500707.
272. Tosi G, Mohiyaddin FA, Schmitt V, et al. Silicon quantum processor with robust long-distance qubit couplings. *Nat Commun*. 2017;8(1):1-11.
273. Pica G, Lovett BW, Bhatt RN, Schenkel T, Lyon SA. Surface code architecture for donors and dots in silicon with imprecise and nonuniform qubit couplings. *Phys Rev B*. 2016;93(3):035306.
274. Morello A, Pla JJ, Zwanenburg FA, et al. Single-shot readout of an electron spin in silicon. *Nature*. 2010;467(7316):687-691.
275. Pla JJ, Tan KY, Dehollain JP, et al. A single-atom electron spin qubit in silicon. *Nature*. 2012;489(7417):541-545.
276. Pla JJ, Tan KY, Dehollain JP, et al. High-fidelity readout and control of a nuclear spin qubit in silicon. *Nature*. 2013;496(7445):334-338.
277. Weber B, Mahapatra S, Ryu H, et al. Ohm's law survives to the atomic scale. *Science*. 2012;335(6064):64-67.
278. Usman M, Bocquel J, Salfi J, et al. Spatial metrology of dopants in silicon with exact lattice site precision. *Nat Nanotechnol*. 2016;11(9):763-768.
279. He Y, Gorman SK, Keith D, Kranz L, Keizer JG, Simmons MY. A two-qubit gate between phosphorus donor electrons in silicon. *Nature*. 2019;571(7765):371-375.
280. Vernacchia S. Quantum leap: advancing a strategy for quantum computing growth in the Middle East. World Government Summit 2019 in partnership with PwC; 2019. <https://www.pwc.com/m1/en/world-government-summit/documents/wgs-quantum-leap.pdf>
281. Sano Y. Comparison on security of single server and multiple servers blind quantum protocols; 2021. arXiv preprint arXiv:2106.05547.
282. Maiti A. Blind quantum computation review; 2017. https://www.cse.iitk.ac.in/users/amitks/quantum/Maiti_report.pdf
283. Gahi Y, El Alaoui I, Guennoun M. An end to end cloud computing privacy framework using blind processing. *Int J Smart Secur Technol*. 2020;7(1):1-20.
284. Gustiani C, Bandung I. *Blind Oracular Quantum Computation: from Concept to Physical Implementation*. Doctoral dissertation. Universitätsbibliothek der RWTH Aachen; 2020. <http://publications.rwth-aachen.de/record/812041/files/812041.pdf>
285. Almudever CG, Lao L, Xiang F, et al. The engineering challenges in quantum computing. Proceedings of the Design, Automation & Test in Europe Conference & Exhibition (DATE); 2017:836-845; IEEE.
286. Córcoles AD, Kandala A, Javadi-Abhari A, et al. Challenges and opportunities of near-term quantum computing systems; 2019. arXiv:1910.02894.
287. Paler A, Devitt SJ. An introduction into fault-tolerant quantum computing. Proceedings of the 52nd Annual Design Automation Conference; 2015:1-6.
288. Franklin D, Chong FT. Challenges in reliable quantum computing. In: Shukla SK, Bahar RI, eds. *Nano, Quantum and Molecular Computing*. Springer; 2004:247-266.
289. Devitt SJ, Munro WJ, Nemoto K. Quantum error correction for beginners. *Rep Prog Phys*. 2013;76(7):076001.
290. Ho A, McClean J, Ong SP. The promise and challenges of quantum computing for energy storage. *Aust Dent J*. 2018;2(5):810-813.
291. Perdomo-Ortiz A, Benedetti M, Realpe-Gómez J, Biswas R. Opportunities and challenges for quantum-assisted machine learning in near-term quantum computers. *Quantum Sci Technol*. 2018;3(3):030502.
292. Usman M, Wong YZ, Hill CD, Hollenberg LCL. Framework for atomic-level characterisation of quantum computer arrays by machine learning. *npj Comput Mater*. 2020;6(1):1-8.
293. Gill SS, Buyya R. A taxonomy and future directions for sustainable cloud computing: 360 degree view. *ACM Comput Surv*. 2018;51(5):1-33.
294. Ajagekar A, You F. Quantum computing for energy systems optimization: challenges and opportunities. *Energy*. 2019;179:76-89.
295. Toosi AN, Calheiros RN, Buyya R. Interconnected cloud computing environments: challenges, taxonomy, and survey. *ACM Comput Surv*. 2014;47(1):1-47.
296. Cacciapuoti AS, Caleffi M, Tafuri F, Cataliotti FS, Gherardini S, Bianchi G. Quantum internet: networking challenges in distributed quantum computing. *IEEE Netw*. 2019;34(1):137-143.
297. Buyya R, Srirama SN, Casale G, et al. A manifesto for future generation cloud computing: research directions for the next decade. *ACM Comput Surv*. 2018;51(5):1-38.

298. Petschnigg C, Brandstötter M, Pichler H, Hofbaur M, Dieber B. Quantum computation in robotic science and applications. Proceedings of the 2019 International Conference on Robotics and Automation (ICRA); 2019:803-810;IEEE.
299. Schaetz T, Monroe CR, Esslinger T. Focus on quantum simulation. *New J Phys*. 2013;15(8):085009.
300. Ott D, Peikert C. Identifying research challenges in post quantum cryptography migration and cryptographic agility; 2019. arXiv:1909.07353.
301. Frolov AV. Can a quantum computer be applied for numerical weather prediction? *Russ Meteorol Hydrol*. 2017;42(9):545-553.
302. Barz S, Kashefi E, Broadbent A, Fitzsimons JF, Zeilinger A, Walther P. Demonstration of blind quantum computing. *Science*. 2012;335(6066):303-308.
303. Xin T, Huang S, Lu S, et al. NMRCloudQ: a quantum cloud experience on a nuclear magnetic resonance quantum computer. *Sci Bull*. 2018;63(1):17-23.
304. Yung MH, Cheng B. Anti-forging quantum data: cryptographic verification of quantum cloud computing; 2020. arXiv:2005.01510.
305. Zhou L, Wang Q, Sun X, Kulicki P, Castiglione A. Quantum technique for access control in cloud computing II: encryption and key distribution. *J Netw Comput Appl*. 2018;103:178-184.
306. Caleffi M, Cacciapuoti AS, Bianchi G. Quantum internet: from communication to distributed computing! Proceedings of the: Proceedings of the 5th ACM International Conference on Nanoscale Computing and Communication; 2018:1-4.

How to cite this article: Gill SS, Kumar A, Singh H, et al. Quantum computing: A taxonomy, systematic review and future directions. *Softw: Pract Exper*. 2022;52(1):66-114. doi: 10.1002/spe.3039