1. Introduction

Quantum computing technology offers fundamentally different solutions to computational problems and enables more efficient problemsolving than what is possible with classical computations. The experimental results are promising, and quantum computers may be available commercially within a few years [[1](#_bookmark36) [10](#_bookmark45)]. One of the most famous algorithms that demonstrate the power of quantum computers is Shors prime factorization algorithm [[11](#_bookmark46)]. The difference between the power of classical and quantum computing is demonstrable via the breaking speed of the Rivest Shamir Adleman (RSA) algorithm [[12](#_bookmark47)]. Solving this computational problem requires billions of years in a traditional computational setting, while in theory, a quantum computer can solve it within a few hours [[11](#_bookmark46),[13](#_bookmark48)]. In 1994, this algorithm caused the big bang of quantum computations and paved the way for the development of quantum computing technology and the evaluation of quantum computers [[14](#_bookmark49)]. Quantum computers integrate several different elements from a functional point of view, such elements are similar to traditional functional ones (registers, gates, memories, buses, CPUs, storage devices), but in the physical layer, the structures of classical and quantum devices are fundamentally different. In a quantum computational framework, the quantum operations are applied on quantum registers. In the quantum register, quantum states formulate quantum superposition, while in a quantum circuit, the quantum states are entangled. These phenomena lead to a fundamentally different system characteristic than what is present in a traditional computer. Besides these, quantum hardware restrictions such as the nocloning theorem also require different circuit design technologies since a quantum state cannot be simultaneously present in more than one quantum gate [[5](#_bookmark40),[10](#_bookmark45)]. A quantum computer has reversible quantum gates that perform a unitary operation on the quantum systems. Quantum computers are working today, but currently we have only a few quantum computer devices in a laboratory environment [[1](#_bookmark36),[3](#_bookmark38) [8](#_bookmark43)]. However, several new fields and interesting results have recently emerged that can significantly boost these developments. The largescale quantum computers are realized in a distributed setting, where smaller quantum computers communicate with one another via a quantum bus. These physically large quantum computers can also be shrunken into smallsized devices via new technologies in the next few years. The situation is very similar to the evolution phases of classical computers both in size and

performance.

The most recent research papers and results of quantum computation technology are reviewed here. All sections also address the open problems of the field. Stateofthe art references are summarized in the *Related Work* subsection at the end of each section.

The novel contributions of our manuscript are as follows:

This paper is organized as follows. In Section [2](#_bookmark8), we review the fundamentals of quantum computations. In Section [3](#_bookmark12), we discuss the basic quantum hardware elements. In Section [4](#_bookmark21), we review the results of largescale quantum computations. In Section [5](#_bookmark27), quantum algorithm implementations are summarized. Finally, in Section [6](#_bookmark34), we conclude the paper.

## Quantum computations

Quantum computers are based on the fundamental concept of quantum information. In these computers, information is represented by quantum states, and with the exploitation of quantum effects provided by quantum mechanics (such as quantum superposition, quantum entanglement, quantum interference, the nocloning theorem, decoherence [[14](#_bookmark49) [18](#_bookmark52)] etc.), quantum computations can be performed in a quantum computer. In the physical layer, quantum systems can manifest in several different ways (atom energy levels, spin, polarization). A general quantum system refers to a *d*dimensional quantum system (for a qubit system, *d* 2), and therefore, a quantum register (a set of *n* quantum states) in a superposition allows us to represent *dn* possible classical values simultaneously. In quantum circuit computations, the quantum states are naturally modeled as entangled systems; thus, the state of each quantum system depends on the other.

=

Quantum computations are based on the fundamental concept of reversible computation. In theory, in a reversible computation, the complete initial state can be recovered from the output state [[19](#_bookmark53)]. Reversible circuits can also be designed for classical systems [[20](#_bookmark54)] such that the number of inputs and outputs of a reversible gate must be equal, and the mapping of a particular input onto a given output must be onetoone. These rules must also be satisfied for a quantum computation system; thus, the input quantum states of a quantum circuit evolve reversibly via unitary operations. Practically, such reversibility is achieved by a series of quantum gates (for example, applying a second NOT gate

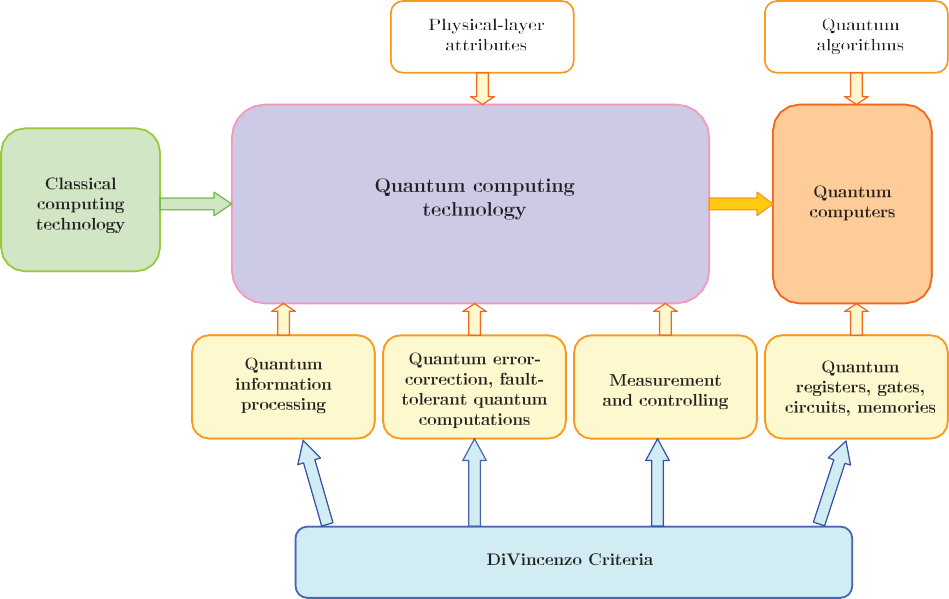
a quantum gate that negates the input on the output of the first NOT gate recovers the original input, etc.). The temporary quantum systems in a quantum computation setting are called ancilla states, which are neglected as the output is realized. Finally, a measurement is applied on the quantum register to extract a classical numerical value for further calculations.

Quantum algorithms utilize the fundamentals of quantum computational complexity. Several quantum algorithms have been proposed so far, whose general conclusion is that utilizing the effects of quantum mechanics would result in a significant speedup (exponential, polynomial, superpolynomial) over the classical algorithms. Besides this (as demonstrated in the prime factorization problem), it is implied that several problems currently intractable via classical algorithms can be solved via quantum algorithms.

For the basic requirements on the physical implementations of quantum computers, the DiVincenzo criteria [[21](#_bookmark55)] establish the fundamental guidelines. These criteria imply the requirement of extensible quantum registers, the initialization of the quantum registers to a known state, the requirement of a universal gate set to run arbitrary quantum algorithms on the quantum computer, and requirements on the coherence time and fidelity to perform long processes, and the results of the quantum computations have to be extractable from the quantum computer via measurements. These are the fundaments of the practical implementation of any quantum computation.

The conceptual diagram of the evolution of quantum computing technology is depicted in [Fig. 1](#_bookmark9). In the functional layer, the aims of classical and quantum computation technology are similar, but in the physical layer, these fields are completely different. The physical foundations of quantum computing technologies are laid down by the DiVincenzo criteria, which are supplemented with particular physical layer attributes. From quantum computing technology, quantum computers are derived with particular conditions on the physical layer attributes of quantum registers, gates, circuits, and memories

The problem of quantum computational complexity has been analyzed from several different aspects. In [[22](#_bookmark56)], the authors studied the computational complexity of linear optics and provided new



**Fig. 1.** The conceptual diagram of the evolution of quantum computing technology from classical computing technology. Quantum computers employ the results integrated by quantum computing technologies.

evidence that quantum computers cannot be efficiently simulated by classical computers. The authors also defined a model of computation in which identical photons are generated, sent through a linearoptical network, and then nonadaptively measured to count the number of photons in each mode. They also studied the prospects for realizing the model using current photonics and optics technology. The authors concluded that the proposed model can solve sampling problems and search for problems that are classically intractable.

Aaronson in [[23](#_bookmark57)] studied the socalled learnability of quantum states. As shown in this work, a quantum state can be characterized by using a number of measurements that grows only linearly with the number of quantum states. The author analyzed the complexity of quantum tomography and showed the possibility of a new simulation of quantum oneway communication protocols by the framework. The paper also analyzed the problem of using a trusted classical advice to verify an untrusted quantum advice.

* 1. *Related work*

For some books on the fundamentals of quantum computations and information, see [[17](#_bookmark51)] and [[14](#_bookmark49),[15](#_bookmark50)], while for the main attributes of quantum communication networks, see [[9](#_bookmark44)]. Deutschs fundamental article on quantum theory and the universal quantum computer can be found in [[24](#_bookmark58)]. For Feynmans article on the question of simulating quantum computations with traditional computers, see [[25](#_bookmark59)]. For the details of the socalled nocloning theorem, see [[26](#_bookmark60)]. For quantum computation problems, see [[27](#_bookmark61)]. For a study on the methods and attributes of maintaining coherence in quantum computers, see Unruhs paper from 1995 [[28](#_bookmark62)]. For a fundamental work on quantum coding, see [[29](#_bookmark63)]. For a discussion of the strengths and weaknesses of quantum computing, see [[30](#_bookmark64)]. A fundamental article on quantum complexity theory is found in [[31](#_bookmark65)]. For DiVincenzos seminal paper on quantum computations from 2000, see [[21](#_bookmark55)]. For Shors major study on prime factorization by a quantum computer, see [[11](#_bookmark46)]. A great review on quantum algorithms can be found in [[32](#_bookmark66)]. For a study on quantum algorithms for algebraic problems, see [[33](#_bookmark67)]. For a paper on some recent progress in quantum algorithms, see [[34](#_bookmark68)]. An account of the role of entanglement in quantumcomputational speedup can be found in [[35](#_bookmark69)]. For a study on matrix product states, projected entangled

pair states, and variational renormalization group methods for quantum spin systems, see [[36](#_bookmark70)]. For an examination of the problem of temporally unstructured quantum computation, see [[37](#_bookmark71)]. The topic of universal blind quantum computation is discussed in [[38](#_bookmark72)]. The problem of multiparty delegated quantum computing is reviewed in [[39](#_bookmark73)]. For a survey on the subject of quantum simulation, see [[40](#_bookmark74)].

## Building blocks of quantum computers

To discuss the most recent updates regarding the fundamental building blocks of quantum computers, we use the following classification: quantum gates, quantum memories, quantum CPUs, quantum controlling and measurement, and quantum errorcorrection tools.

* 1. *Quantum gates*

The quantum gates of a quantum computer perform unitary operations on quantum states. The Toffoli and Fredkin quantum gates [[14](#_bookmark49),[15](#_bookmark50),[17](#_bookmark51) [19](#_bookmark53)] are threebit gates and are essential since any quantum circuit can be decomposed into a set of Toffoli gates or Fredking gates and can also simulate NOT or CNOT (ControlledNOT) gates. In other words, either gate can be used to realize universal quantum computations [[18](#_bookmark52)]. Since quantum gates are reversible, the ancilla states are cleared, and only the valuable outputs are kept.

In the physical layer, the quantum gates can be realized by ion traps, superconductors, linear optic tools, diamonds, quantum dots, donorbased systems, or topological quantum computing elements, see the related references in the Related Work subsection. Handling the errors of the quantum gates for practical implementations requiring efficient quantum errorcorrection codes is still an open problem [[8](#_bookmark43),[10](#_bookmark45),[41](#_bookmark75) [52](#_bookmark86)].

In [[53](#_bookmark87)] the authors studied the achievable quantum advantages with shallow circuits. As the authors have found the constantdepth quantum circuits are more powerful than their classical counterparts. As the authors concluded that any classical probabilistic circuit that solves that particular problem must have depth logarithmic in the number of input quantum states. The authors also found that this problem can be solved with unit certainty

by a constantdepth quantum circuit. This quantum circuit has to contain only oneand twoqubit gates acting locally on a twodimensional grid, which represents a practically implementable gate model structure.

In [[54](#_bookmark88)], the authors studied the power of IQP (instantaneous quantum polynomialtime) circuits in the presence of some physically motivated constraints. The results are particularly important, since it is hard to simulate classically an IOP circuit. In this work the authors found that there exists a family of IQP circuits that can be implemented on a square lattice of *n* qubits with a particular depth. They also found that if an arbitrarily small constant amount of noise is added to each qubit there exists a polynomialtime classical algorithm that can simulate sampling from the resulting distribution.

In [[55](#_bookmark89)], the authors studied the design methods of highfidelity threequbit gates (Toffoli, ControlledNotNot and Fredkin), These quantum gates are particularly important for quantum error correction and experimental quantum information processing. The proposed model is based on the fundamentals of machinelearning. As the authors have found, the procedures are applicable to a system comprising three nearestneighborcoupled superconducting artificial atoms. The authors concluded that the proposed scheme achieves 99.9% fidelity. This result is particularly convenient since it is a threshold fidelity for faulttolerant quantum computing.

* 1. *Quantum memories*

In quantum circuit computations, quantum memories are formulated by *n* stationary quantum states. The quantum memories store these quantum systems in a quantum register for information processing.

Several different concepts exist in the literature for the realization of quantum memories. An interesting approach is topological quantum memory [[56](#_bookmark90)], which is achieved via an array or torus of quantum states. These quantum systems are entangled in some patterns to formulate a stable logical quantum system.

Regarding the physical implementations of quantum memories, improving the memory lifetimes are still an open problem [[8](#_bookmark43),[57](#_bookmark91) [64](#_bookmark98)], however the results are encouraging. A roomtemperature quantum bit memory exceeding one second has been demonstrated in [[60](#_bookmark94)], while in [[61](#_bookmark95)], a largescale quantumcomputer architecture has been proposed with atomic memory and photonic interconnects.

For the discussion on quantum random access memory, see [[59](#_bookmark93)]. As the authors defined, a quantum random access memory (qRAM) uses *n* qubits to address any quantum superposition of *N* memory cells. The authors proposed an architecture that exponentially reduces the requirements for a memory call. As the authors found, the results allows to construct a more robust qRAM algorithm and also leads to an exponential decrease in the power needed for addressing. The work concluded with a quantum optical implementation.

The exponential capacity of associative memories under quantum annealing recall is studied in [[65](#_bookmark99)]. In this work the authors showed that using quantum annealing for recall tasks endows associative memory models (that models can store a sublinear number of memories in some theoretical models) with exponential storage capacities. The authors also demonstrated the application of their scheme via the Dwave processor that provided a programmable quantum annealing device.

The optimization of dynamical decoupling for quantum memory via recurrent neural networks is studied in [[57](#_bookmark91)]. In this work the authors utilized the methods of traditional machine learning that are based on recurrent neural networks to optimize dynamical decoupling sequences. As the authors note, these decoupling method is a relatively simple technique for suppressing the errors

in quantum memory. The authors showed that at the present of some prior knowledge and with some conditions on the iteration procedure, the analyzed models are useful for error correction in quantum memories.

In [[66](#_bookmark100)] a definition of quantum memristors (resistors with memory whose resistance depends on the history of the crossing charges) is included. The decoherence mechanism in the proposed model is controlled by a continuousmeasurement feedback scheme. The authors also demonstrated that memory effects actually persist in the quantum regime, and the superconducting circuits are ideal for their practical implementation. As the authors concluded, the introduced model of quantum memristor can be used as a building block for neuromorphic quantum computations, and quantum simulations of nonMarkovian systems. The quantum memristors are resistive quantum elements retaining information of their past dynamics [[67](#_bookmark101)]. In [[67](#_bookmark101)], the authors analyzed the quantum memristors implementations using superconducting circuits. The authors introduced a quantum device whose memristive behavior arises from quasiparticleinduced tunneling when supercurrents are canceled. As the authors have introduced a model for the quantification of quantum memory retention, and concluded the hysteretic behavior is achievable via currently implementable measurement procedures in superconducting quantum circuits. In [[68](#_bookmark102)], an analysis of qubitbased memcapacitors and meminductors is proposed. As the authors found, the capacitive and inductive devices offer remarkable functionalities for quantum computations (superconducting charge and phase qubits are quantum versions of memory capacitive and inductive systems). As it is shown in this work, the qubitbased memcapacitors and meminductors exhibit unusual hysteresis curves for some special inputs. As a main result of this paper, the set of known memcapacitive and meminductive systems can be extended to qubitbased quantum devices.

* 1. *Quantum CPUs*

Quantum CPUs use a quantum bus for the communication between the functional elements of a quantum computer. From a computing perspective, quantum CPUs can be approached through the building blocks that formulate it: quantum adders. Several different reversible quantum adder types have been defined, see quantum Fouriertransformbased adders, lineartime adders, quantum carrysave adders, carrylookahead adders, conditionalsum adders, quantum carryselect adders, quantum carryripple adders [[19](#_bookmark53)] to realize quantum computations in different architectural models. The quantum versions of the classical adders can also be made for quantum computations, with reversible structure and parallel implementations. The quantum adders are all reversible and use ancilla quantum states, but they are equipped with different working mechanisms, circuit depths, latencies, and performance; thus, the realization of their cooperation brings up several open problems [[69](#_bookmark103) [77](#_bookmark111)].

For the parallelization of the quantum circuits, two basic networks models were defined in [[19](#_bookmark53)]. The first network model allows longdistance communication between a set of quantum states (set of states that are involved in the quantum computations). Meanwhile, the second model allows only local communications; it is precisely possible only between the nearest neighbors in a linear layout [[9](#_bookmark44),[19](#_bookmark53)]. The performance of the various quantum adders was characterized in these network models, and it has been concluded that the performance of the different configurations is close to each other. For the implementation of the quantum communications between the quantum CPU and the functional elements of the quantum computer, the different experimental quantum errorcorrection methods can be used [[19](#_bookmark53)]. By theory, the performance of

a quantum circuit is denoted by *O ()*, and because of the nature of

signal propagations, the latency of any circuit is limited to *n* in an *n*bit system, and with *D*dimensional structure (practically, *D* 3).

=

( )*O*

In [[19](#_bookmark53)], five different qubus interconnect topologies were analyzed using Shors prime factorization algorithm. For the basic gate structure of the quantum prime factorization algorithm, see [Fig. 2](#_bookmark17). The quantum algorithm aims to increase the probabilities of the solutions (red dots) in the quantum register *A*.

As it has been concluded in [[19](#_bookmark53)], the quantum carryripple adder provides the best performance for a wide range of parameters. As it is concluded in this work, the small nodes (up to five logical qubits) and a linear interconnection network provide adequate performance; more complex networks are unnecessary as the number of bits of the factorized number reaches several hundred bits. Regarding the performance of these quantum adders, in this work it also has been concluded that these adders makes possible to factorize a 6000bit number one million times and thirteen thousand times faster than it is possible by the BCDP (Beckman Chari Devabhaktuni Preskill) modular exponentiation algorithm.

In [[70](#_bookmark104)] the authors also studied the properties of quantum adders, specifically the method of protected state transfer using an approximate quantum adder. In this work the authors defined a decoherence protected protocol for transmitting photonics quantum states over depolarizing quantum channels. The studied protocol was implemented by an approximate quantum adder engineered through spontaneous parametric down converters. As the authors concluded a higher success probability can be achieved via the method than by distilled quantum teleportation protocols for distances below a threshold. In [[72](#_bookmark106)], the authors studied the approximate quantum adders with genetic algorithms. Particularly, the authors proposed the theoretical aspects of approximate quantum adders, and defined an optimization method that is based on genetic algorithms. As the authors have found the results makes possible to improve the achievable efficiency and fidelity of some previous protocols. The authors practically implemented an approximate quantum adder using the IBM Quantum Experience. As the authors concluded the approximate quantum adders can help to enhance quantum information processing.

In [[78](#_bookmark112)], a method for quantum state transfer via noisy photonic and phononic waveguides is studied. The authors defined a protocol in which a quantum state of photons stored in a first cavity can be faithfully transferred to a second distant cavity via an infinite onedimensional waveguide. As the authors found this transfer is possible while the transferred information being immune to arbitrary noise (e.g. thermal noise) injected into the waveguide. The authors also studied a cavity QED setup, where atomic ensembles, or single atoms represented the quantum memory. As the authors concluded the proposed models and results can be applied in the various fields of phononic quantum information processing.

In [[71](#_bookmark105)], the authors studied the realization of quantum autoencoders using quantum adders with genetic algorithms. As the authors stated, there exists a useful connection between approximate quantum adders and quantum autoencoders. As the authors found, it is possible to develop optimized approximate quantum adders using genetic algorithms. As the authors have concluded, the results also have several practical consequences, since quantum autoencoders can be implemented for a variety of initial states, and quantum autoencoders can be designed via controllable quantum platforms.

In [[73](#_bookmark107)], the authors studied the problem of spaceefficient design for reversible floating point adder in quantum computing. As the authors emphasized, reversible logic has crucial significance in experimental lowpower computing and quantum computing. The authors defined a spaceefficient reversible floatingpoint adder for quantum computers. The proposed model can be used for

binary quantum computation, and to improve the designs of the expensive units. The authors proposed techniques for the cost reduction, and for the faulttolerant designs for the circuits.

In [[79](#_bookmark113)], the competing and cooperating technological trends related to experimental quantum computing and quantum computer implementations are studied. As it is concluded here, classical computers will still play a relevant part, however the classical computations are limited by thermodynamics and by the nature of atomic matter and quantum effects.

* 1. *Controlling and measurement*

The appropriate control mechanisms are a necessity for quantum state manipulations, readout, errorcorrection processes, and faulttolerant quantum computations.

Relevant progress has been made since the ion trapbased implementations [[10](#_bookmark45),[61](#_bookmark95),[80](#_bookmark114) [90](#_bookmark124)], such as superconducting quantum circuits [[1](#_bookmark36),[4](#_bookmark39),[8](#_bookmark43),[42](#_bookmark76),[67](#_bookmark101),[91](#_bookmark125) [97](#_bookmark131)], linear optics [[10](#_bookmark45),[98](#_bookmark132) [118](#_bookmark152)], topological

quantum computing [[43](#_bookmark77),[47](#_bookmark81),[52](#_bookmark86),[119](#_bookmark153) [130](#_bookmark164)], quantum dots [[75](#_bookmark109),[77](#_bookmark111), [131](#_bookmark165) [138](#_bookmark172)], donorbased quantum implementations [[10](#_bookmark45),[62](#_bookmark96),[69](#_bookmark103),[138](#_bookmark172) [146](#_bookmark179)], anyonbased quantum computing [[10](#_bookmark45),[96](#_bookmark130),[123](#_bookmark157),[126](#_bookmark160),[130](#_bookmark164),[147](#_bookmark181), [148](#_bookmark182)], and others (see Related Works).

An important open problem in this fields is the preparation of quantum systems for the computations [[149](#_bookmark183) [153](#_bookmark187)], as well as the experimental realization of the measurements [[48](#_bookmark82),[49](#_bookmark83),[101](#_bookmark135),[113](#_bookmark147), [154](#_bookmark188) [164](#_bookmark198)] that extracts valuable information from the quantum states.

In [[151](#_bookmark185)] the authors studied the practical superposing of two pure quantum states with partial prior knowledge. The results are particularly important in experimental quantum information processing since generating superposition of any two unknown pure states is a challenge since it can be achieved only with some prior knowledge about the input states but only in a probabilistic way. The apriori knowledge is represented by the overlap between the two unknown states with respect to some given referential state. In [[151](#_bookmark185)], the authors implemented the probabilistic protocol of superposing two pure states in a threequbit nuclear magnetic resonance system. They also studied the feasibility of the protocol by preparing a families of input states, and determined the average fidelity between the prepared state. Since the achieved fidelity was high, the authors have also concluded that the proposed implementation can be extended to more complex situations and to complex quantum circuits.