A review on Quantum Machine Learning and Quantum Cryptography*

1st Mauricio Solar
Dept. of Informatics
Universidad Tecnica Federico Santa Maria (UTFSM)
Santiago, Chile
mauricio.solar@usm.cl or ORCID

2nd Felipe Cisternas Alvarez
Dept. of Informatics
Universidad Tecnica Federico Santa Maria (UTFSM)
Valparaiso, Chile
felipe.cisternasal@sansano.usm.cl

3rd Jean-Pierre Villacura
Dept. of Informatics
Universidad Tecnica Federico Santa Maria (UTFSM)
Valparaiso, Chile
jean-pierre.rojas@sansano.usm.cl

4th Liubov Dombrovskaia
Informatique Dept. (of Aff.)
UTFSM (of Aff.)
Santiago, Chile
liuba@inf.utfsm.cl or ORCID

Abstract—This article corresponds to an extensive review of Quantum Computers. We chose to consider topics relevant to quantum computing, such as machine learning, and the deepening of other issues related to cybersecurity. We introduce the reader to the basic concepts of quantum computing so that they can easily understand the terms mentioned in this review. We analyze different state of the art articles, and we give a summary of the contributions made. Finally we conclude with the analysis of the bibliography, the research centers, the current state of the art, surprising results and conclusions.

Index Terms—quantum machine learning, quantum key distribution, quantum cryptography

I. Introduction

With certainty it can be stated that today's computers are much faster than the computers of 70 years ago. The computers of that time were large, heavy, with a very limited capacity and processing speed compared to what is the standard now a day. We could consider quantum computers to be in this same state, as an emerging technology that is still expensive, bulky and with a lot of research potential [1].

The theory of quantum computing points out that its processing speed can be much faster than even the fastest supercomputer today. Examples such as Shor's algorithm with its potential ability to factor large prime numbers in a matter of seconds, as opposed to the thousands of years that classical computing could take, are considered signs of the advances and development that is to come with quantum computing [2].

This paper explores a range of subjects concerning quantum computing, including quantum computers and technologies. It is structured to provide readers with a comprehensive understanding, starting from the basics of quantum computing and progressing to cover a wide range of proposed models for quantum computers. Additionally, the paper delves into the future prospects and developments of the fields Quantum Machine Learning (QML) and Quantum Cryptography, highlighting the immense potential of quantum computing and discussing current advancements.

The structure of this paper after this introduction includes a brief overview of Quantum Computing (Quantum Computers and Technologies, Quantum Data, Quantum Gates, Noise, Quantum Error Correction Quantum Cybersecurity, and Quantum Machine Learning). In the section State of the Art we show the methodology, we describe the new works and research, we show a comparative analysis of the latest advances, a bibliographic discussion and we show a state of the art timeline jointly with expected or surprising results. The final section summarizes the conclusions of this work.

II. Brief overview of Quantum Computing

A. Quantum Computing

Quantum computing relies on properties of quantum mechanics to compute problems that would be out of reach for classical computers. A Quantum Computer (QC) uses qubits. Qubits are like regular bits in a classical computer, but with the added ability to be put into a superposition state and share entanglement with one other [22].

A QC works using quantum principles. Quantum principles require a new dictionary of terms to be fully understood, terms that include superposition, entanglement, and decoherence. Let's explain these principles below.

- Superposition: Superposition states that, much like waves in classical physics, you can add two or more quantum states and the result will be another valid quantum state. Conversely, you can also represent every quantum state as a sum of two or more other distinct states. This superposition of qubits gives QCs their inherent parallelism, allowing them to process millions of operations simultaneously.

- Entanglement: Quantum entanglement occurs when two systems link so closely that knowledge about one gives you immediate knowledge about the other, no matter how far away they are. Quantum processors can draw conclusions about one particle by measuring another one, Quantum entanglement allows QCs to solve complex problems faster. When a quantum state is measured, the wavefunction collapses and you measure the state as either a zero or a one. In this known or deterministic state, the qubit acts as a classical bit. Entanglement is the ability of qubits to correlate their state with other qubits.
- Decoherence: Decoherence is the loss of the quantum state in a qubit. Environmental factors, like radiation, can cause the quantum state of the qubits to collapse. A large engineering challenge in constructing a QC is designing the various features that attempt to delay decoherence of the state, such as building specialty structures that shield the qubits from external fields.

The current state of quantum computing is referred to as the noisy intermediate-scale quantum (NISQ) era [8], characterized by quantum processors containing 50–100 qubits which are not yet advanced enough for fault-tolerance or large enough to achieve quantum supremacy, the term NISQ was coined by [20]. These processors, which are sensitive to their environment (noisy) and prone to quantum decoherence, are not yet capable of continuous quantum error correction. This intermediate-scale is defined by the quantum volume, which is based on the moderate number of qubits and gate fidelity.

Classical computers perform deterministic classical operations or can emulate probabilistic processes using sampling methods. By harnessing superposition and entanglement, QCs can perform quantum operations that are difficult to emulate at scale with classical computers. Ideas for leveraging NISQ quantum computing include optimization, quantum simulation, cryptography, and Machine Learning (ML).

Notably, QCs are believed to be able to solve many problems quickly that no classical computer could solve in any feasible amount of time—a feat known as quantum supremacy.

B. QCs and technologies

A QC is a computer that exploits quantum mechanical phenomena. At small scales, physical matter exhibits properties of both particles and waves, and quantum computing leverages this behavior using specialized hardware. Classical physics cannot explain the operation of these quantum devices, and a scalable QC could perform some calculations exponentially faster than any modern classical.

No one has shown the best way to build a fault-tolerant QC, and multiple companies and research groups are investigating different types of qubits. We give a brief example of some of these qubit technologies below.

- Gate-based ion trap processors: Trapped ion QCs implement qubits using electronic states of charged atoms called ions. The ions are confined and suspended above the microfabricated trap using electromagnetic fields. Trapped-ion based systems apply quantum gates using lasers to manipulate the electronic state of the ion [30]. Trapped ion qubits use atoms that come from nature, rather than manufacturing the qubits synthetically [31].
- Gate-based superconducting processors: Superconducting quantum computing is an implementation of a QC in superconducting electronic circuits. Superconducting qubits are built with superconducting electric circuits that operate at cryogenic temperatures [32].
- Photonic processors: A quantum photonic processor is a device that manipulates light for computations. Photonic QCs use quantum light sources that emit squeezed-light pulses, with qubit equivalents that correspond to modes of a continuous operator, such as position or momentum [33].
- Neutral atom processors: Neutral atom qubit technology is similar to trapped ion technology. However, it uses light instead of electromagnetic forces to trap the qubit and hold it in position. The atoms are not charged and the circuits can operate at room temperatures [34]. QuEra has a publicly-accessible neutral-atom computer (https://www.quera.com). It is a 256-qubit QC based on programmable arrays of neutral Rubidium atoms, trapped in vacuum by tightly focused laser beams.
- Rydberg atom processors: A Rydberg atom is an excited atom with one or more electrons that are further away from the nucleus, on average. Rydberg atoms have a number of peculiar properties including an exaggerated response to electric and magnetic fields, and long life. When used as qubits, they offer strong and controllable atomic interactions that you can tune by selecting different states [35].
- Quantum annealers: Quantum annealing uses a physical process to place a quantum system's qubits in an absolute energy minimum. From there, the hardware gently alters the system's configuration so that its energy landscape reflects the problem that needs to be solved. The advantage of quantum annealers is that the number of qubits can be much larger than those available in a gate-based system. In fact, Quantum annealing is implemented in D-Wave's generally available QCs, such as the Advantage™ https://www.dwavesys.com, enabling the creation of Quantum Processing Units (QPUs) with more than 1200 qubits, far beyond the state of the art for gate-model quantum computing. However, their use is limited to specific cases only [36].

C. Quantum Data

Quantum data is any data source that occurs in a natural or artificial quantum system. Quantum data exhibits superposition and entanglement, leading to joint probability distributions that could require an exponential amount of classical computational resources to represent or store. The quantum supremacy experiment showed it is possible to sample from an extremely complex joint probability distribution of 2^{53} Hilbert space.

The qubit serves as the basic unit of quantum information. It represents a two-state system, just like a classical bit, except that it can exist in a superposition of its two states. In one sense, a superposition is like a probability distribution over the two values. However, a quantum computation can be influenced by both values at once, inexplicable by either state individually. In this sense, a superposed qubit stores both values simultaneously. When measuring a qubit, the result is a probabilistic output of a classical bit. If a QC manipulates the qubit in a particular way, wave interference effects can amplify the desired measurement results.

The quantum data generated by NISQ processors are noisy and typically entangled just before the measurement occurs. Heuristic ML techniques can create models that maximize extraction of useful classical information from noisy entangled data.

The following are examples of quantum data that can be generated or simulated on a quantum device:

- Chemical simulation: Extract information about chemical structures and dynamics with potential applications to material science, computational chemistry, computational biology, and drug discovery [37].
- Quantum matter simulation: Model and design high temperature superconductivity or other exotic states of matter which exhibits many-body quantum effects [38].
- Quantum control: Hybrid quantum-classical models can be variationally trained to perform optimal open or closed-loop control, calibration, and error mitigation. This includes error detection and correction strategies for quantum devices and quantum processors [39].
- Quantum communication networks: Use ML to discriminate among non-orthogonal quantum states, with application to design and construction of structured quantum repeaters, quantum receivers, and purification units [40].
- Quantum metrology: Quantum-enhanced high precision measurements such as quantum sensing and quantum imaging are inherently done on probes that are small-scale quantum devices and could be designed or improved by variational quantum models [41].

D. Quantum Gates

The state of qubits can be manipulated by applying quantum logic gates, analogous to how classical bits can be manipulated with classical logic gates. Unlike many classical logic gates, quantum logic gates are reversible [6]. Quantum logic gates are represented by unitary matrices, a gate which acts on n qubits is represented by $2^n \times 2^n$ unitary matrix.

Quantum states are typically represented by kets, from a notation know as bra-ket, the vector representation of a single qubit is shown in equation 1.

$$|a\rangle = v_0|0\rangle + v_1|1\rangle \rightarrow \begin{bmatrix} v_0 \\ v_1 \end{bmatrix} \tag{1}$$

Here v_0 and v_1 are the complex probability amplitudes of the qubit, these values determine the probability of measuring a 0 or a 1, when measuring the state of the qubit. The value zero is represented by the ket in equation 2, and the value one is represented by the ket in equation 3.

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \tag{2}$$

$$|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \tag{3}$$

The tensor product denoted by the symbol $\otimes$, is used to combine quantum states. The action of the gate on a specific quantum state is found by multiplying the vector $|\phi_1\rangle$ which represents the state by the matrix U representing the gate, thus the result is a new quantum state $|\phi_2\rangle$ shown in equation 4.

$$U|\phi_1\rangle = |\phi_2\rangle \tag{4}$$

There exist many number of quantum gates, below we review some of the most often used in the literature:

- NOT Gate: This gate is widely known as X-Pauli gate, as this particular quantum gate transforms the existing state of the qubit to be rotated around the X-axis. As the name suggests, the NOT gate would convert a qubit from its initial state to its complement state. This quantum gate is represented by the matrix in equation 5, and operates as shown in equation 6.

$$X := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \tag{5}$$

$$X|0\rangle = |1\rangle \text{ and } X|1\rangle = |0\rangle \tag{6}$$

- Y-Pauli Gate: The Y-Pauli gates are capable of rotating the input qubit around the Y-axis. This quantum gate is represented by the matrix in equation 7, and operates as shown in equation 8.

$$Y := \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \tag{7}$$

$$Y|0\rangle = i|1\rangle \text{ and } Y|1\rangle = -i|0\rangle \tag{8}$$

- Z-Pauli Gate: The Z-Pauli or phase flip gate are capable of rotating the input qubit around the Z-axis. This quantum gate is represented by the matrix in equation 9.

$$Z := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{9}$$

Pauli Z leaves the biasis state $|0\rangle$ unchanged and maps $|1\rangle$ to $-|1\rangle$ as shown in equation 10.

$$Z|0\rangle = |0\rangle \text{ and } Z|1\rangle = -|1\rangle \tag{10}$$

- Controlled NOT Gate: the Controlled NOT (CNOT) gate acts on 2 (or more) qubits, and performs the NOT operation on the second (or more) qubit only when the first qubit is $|1\rangle$, this gate is represented by the Hermitian unitary matrix (equation 11), and operates as in equation 12.

$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \tag{11}$$

$$\begin{aligned} CNOT|00\rangle &= |00\rangle \\ CNOT|01\rangle &= |01\rangle \\ CNOT|10\rangle &= |11\rangle \\ CNOT|11\rangle &= |10\rangle \end{aligned} \tag{12}$$

- Hadamard gate: The Hadamard gate, acts on a single qubit and creates an equal superposition states given a biasis state. The Hadamard gate performs a rotation of π bout the axis $(\hat{x} + \hat{z})/\sqrt{2}$ at the Bloch Sphere (Figure 1). This gate is represented by the Hadamard matrix (equation 13), and operates as in equation 14.

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \tag{13}$$

$$\mathrm{H}|0\rangle = \tfrac{|0\rangle+|1\rangle}{\sqrt{2}} \text{ and } H|1\rangle = \tfrac{|0\rangle-|1\rangle}{\sqrt{2}} \tag{14}$$

E. Noise

Noise is present in modern day QCs. Qubits are susceptible to interference from the surrounding environment, imperfect fabrication, TLS and sometimes even gamma rays. Until large scale error correction is reached, the algorithms of today must be able to remain functional in the presence of noise. This makes testing algorithms under noise an important step for validating quantum algorithms and quantum models.

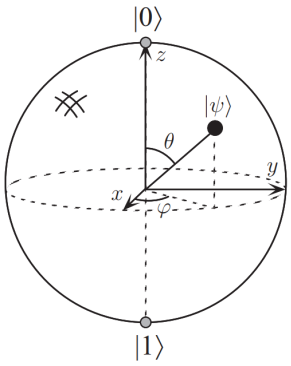

Fig. 1. Bloch sphere to represent a qubit

F. Quantum Error Correction (QEC)

QEC is used in quantum computing to protect quantum information from errors due to decoherence and other quantum noise. Traditional error correction employs over repetition. The repetition code is the simplest but most inefficient way. The idea is to store the information multiple times and take a larger vote in the event that these copies are later found to differ. Copying quantum information is not possible due to the no-cloning theorem. This theorem seems to present an obstacle to formulating a theory of QEC, nevertheless, it is conceivable to transfer the logical information of a single qubit to a highly entangled state of several physical qubits [21].

G. Quantum Cybersecurity

1) Quantum Cryptography: Cryptography has had an important development since 1975 with the establishment of the Data Encryption Standard (DES) algorithm for file encryption while computing was emerging. Since then, several algorithms have been developed to fulfill this cryptographic function, the best known being RSA (Rivest-Shamir-Adleman) and Advanced Encryption Standard (AES).

With the emergence of quantum computing, several researchers comment on the risk that the rise of this paradigm may threaten encryption algorithms based on classical computing, which are considered secure due to the amount of time it takes to test all combinations, easily 50 years using supercomputers. Quantum computing threatens the security of these algorithms by being able to perform calculations much faster. Being able to solve operations that in the classical paradigm would take about 50 years using supercomputers in a matter of seconds.

The state of the art of quantum computing proposes modifications to algorithms RSA [7] and AES [14]:

- [14] proposes a modified AES algorithm comparing different methods of random number generation, resulting in the use of Quantum Random Walk (QRW) the best encryption performance. It is proposed the modifying the Shift row operation introducing

random movements using QRW, making it difficult to predict the correct order during the decryption process. This adds an additional layer of complexity and makes attempts to decrypt encrypted information difficult without proper knowledge of the correct sequence.

- [7] proposes that the little investigation about RSA algorithm in Quantum computing is due to actual limits of Shor's algorithm. They propose a Quantum ring algorithm: GEECM (Grover plus Elliptic-Curve factorization Method using Edwards curves), using pre-quantum algorithm to find small primers and accelerate it with quantum techniques [7].

2) Quantum Key Distribution (QKD): This topic is closely related to cryptography, since the security of the data depends on the transmission of the key previously generated by a cryptographic algorithm.

There are dangers associated with the transmission of the key that were partly solved with the introduction of the asymmetric key (whose most famous algorithm is RSA).

Quantum computing proposes new solutions in this aspect by being able to transmit the same key to two recipients (Alice and Bob), with a very high certainty of corroborating that there is no third person obtaining this key. This is possible due to quantum properties such as entanglement and non-cloning. With entanglement it is possible to know the state of both photons (i.e. direction of spin) and non-cloning allows to detect if there is any intruder in the system, since it would yield a common key different from Alice and Bob (Figure 2.

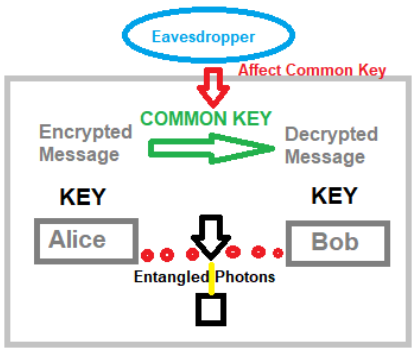

Fig. 2. Quantum Key Distribution (QKD)

Since Alice and Bob have the same common key, Alice can encrypt her message and send it to Bob, who has the key to decrypt and therefore read the message. We assume noise-free channel for this situation.

Quantum computing can also contribute to the 'one-time-pad' problem of classical computing by providing random keys due to the Heisenberg uncertainty principle. Note that in this type of problem security depends to some degree on the randomness of the key.

H. Quantum Machine Learning (QML)

One of the most successful technologies of this century is ML, a subset of Artificial Intelligence (AI) that focuses on developing algorithms and models that enable computers to learn from data and make predictions or decisions without being explicitly programmed.

Like other classical theories, ML and learning theory can in fact be embedded into the quantum mechanical formalism. Formally speaking, this embedding leads to the field known as QML which aims to understand the ultimate limits of data analysis allowed by the laws of physics. While there are similarities between classical and QML, there are also some differences. Because QML employs QCs, noise from these computers can be a major issue.

In ML we have different paradigms that also applies to QML:

- Supervised Learning (Task-based)
- Unsupervised Learning (Data-based)
- Reinforcement Learning (Reward-based)

and there is a bunch of algorithms of QML being researched:

- Quantum Neural Networks (QNNs)
- Quantum Kernels (QKs)
- Variational Quantum Algorithms (VQAs)

1) Quantum Neural Networks (QNNs): A QNN is used to describe a parameterized quantum computational model that is best executed on a QC. This term is often interchangeable with Parameterized Quantum Circuit (PQC). These involve a sequence of unitary gates acting on the quantum data states $|\psi_j\rangle$, some of which have free parameters θ that will be trained to solve the problem.

QNNs are employed in all three QML paradigms mentioned above. For instance, in a supervised classification task, the goal of the QNN is to map the states in different classes to distinguishable regions of the Hilbert space, in the unsupervised learning scenario of a clustering task is mapped onto a MAXCUT problem [16] and solved by training a QNN to maximize distance between classes. Finally, in the reinforced learning task of a QNN can be used as the Q-function approximator [25], which can be used to determine the best action for a learning agent given its current state.

As in classical neural networks, there are different types of networks such as convolutional networks, recurrent networks, etc. their quantum variants have been researched, such as quantum convolutional neural networks [11] and quantum recurrent neural networks [4].

2) Quantum Kernels (QKs): In ML, a kernel is a function that defines the similarity or distance between pairs of data points in a high-dimensional feature space. QK methods consider the computation of kernel functions using QCs.

There are many possible implementations. For example consider a reproducing kernel Hilbert space equal to

the quantum state space, which is finite dimensional. In simpler terms, we can think of the quantum state space as a finite-dimensional space [23]. By using this approach, we can calculate kernel functions within this finite-dimensional space.

Another approach involves studying a reproducing kernel Hilbert space that is infinite-dimensional. In this case, we are transforming classical vectors (which represent data points) using a QC. The QC helps us map these classical vectors into infinite-dimensional vectors, an infinite-dimensional space allows for more complex representations and calculations.

3) Variational Quantum Algorithms (VQAs): VQAs are a hybrid quantum-classical optimization algorithm in which an objective function is evaluated by quantum computation, and the parameters of this function are updated using classical optimization methods [10].

The variational method in quantum theory is a classical method for finding low energy states of a quantum system. The idea of this method is that one defines a wave function (called an ansatz) as a function of some parameters, and then one finds the values of these parameters that minimize the expectation value of the energy.

It has been realized that QCs can mimic the classical technique and that a QC does so with certain advantages [18], [29], when one applies the classical variational method to a system of n qubits, an exponential number of complex numbers is necessary to generically represent the wave function of the system. However, with a QC, one can directly produce this state using a PQC with less than exponential parameters.

4) Inductive Bias: Inductive bias means that any model, can only represent a subset of all possible functions and is naturally inclined towards certain types of functions. These functions relate the input features to the output predictions.

Inductive bias encompasses the assumptions and restrictions made in the model design and optimization process, shaping the search space for potential models. The choice of model parameterization or embedding, as well as techniques like regularization and learning rate modulation, contribute to the inductive bias.

To achieve quantum advantage with QML, we aim for QML models that have an inductive bias that is difficult to simulate efficiently using classical models. Recent research has shown that it is possible to construct QKs with this property, although there are some complexities regarding their trainability.

III. State of the Art

A. Methodology

To gather new information on Quantum Cybersecurity it was used the classical search method with the following set:

- Relevant Topic: Quantum Cybersecurity. Format: Investigation and State of art. Specialized Authors: Abd El-Latif, Ahmed. Time Frame: 2021-2023.
- Keywords: Quantum, post-quantum, Cybersecurity, encryption, Key-Distribution, Authentication, Digital signature, IoT.
- BDB: Web of Science, Springerlink.

Meanwhile, to gather more information on QML, it was used the Snowball methodology, reading the citations of the most recent papers on QML.

B. Related works and Research to QML and Cybersecurity

The related works on cybersecurity reported in the literature is summarized below.

In [14], the authors propose a modified AES algorithm and use quantum computing to encrypt/decrypt AES image files using IBM Qiskit for performance evaluation. They show that AES algorithm can be implemented using quantum gates and suggest that AES be implemented with random number generation.

AES is combined with the use of random number generation in the process. In the traditional implementation of the AES algorithm, the Shift Row operation moves the data to align them at certain encryption steps. Since the decryption process can reverse the order of these steps, it becomes predictable. To address this vulnerability, the author suggests modifying the performance of the Shift Row operation to introduce random movements using Quantum Random Walk (QRW), making it difficult to predict the correct order during the decryption process, achieving greater security than classical approach.

In [26], the authors focus on analyzing characteristics of the quantum cryptography and exploring of the advantages of it in the future internet. They analyze the QKD protocol in the noise-free channel by making measurements of different variables. Probability of the eavesdropper being detected v/s number of photons measured in a noise-free channel and 30% noise. Also analyzes the probabilities of errores in the receiver v/s probability of eavesdropper to eavesdrop on the channel.

In [28], the authors make a contribution in the state of the art of cybersecurity from wide perspectives. They give an overview of quantum computing and how it can affect cybersecurity issues. Also demonstrate solutions in quantum computing to problems in classical computing paradigm related to cybersecurity, and relates how quantum computing could be used in the future to make cybersecurity solutions better.

In [7], the authors make a contribution proposing parameters and changes to RSA to make Key-Generation, encrypt and decryption, signatures and verification feasible in actual computing and, at the same time, protected against quantum computing attacks. They propose a new quantum algorithm to generate factor numbers, GEECM faster than Shor and algorithms of classic paradigm.

In [25], the authors introduce a new training method for PQCs that can be used to solve Reinforcement Learning (RL) tasks for discrete and continuous state spaces based on the deep Q-learning algorithm. They adapt the Deep Q-Network (DQN) algorithm to use a PQC as its Q-function approximator instead of a Neural Network (NN). For this, they use a hardware-efficient ansatz, a target network, an ϵ-greedy policy to determine the agent's next action and experience replay to draw samples for training the Q-network PQC. The Q-network then is $U_\theta(s)$ parametrized by θ and the target network PQC is $\hat{U}_{\theta_\delta}(s)$, where θ_δ is a snapshot of the parameters θ which is taken after fixed intervals of episodes δ and the circuit is otherwise identical to that $U_\theta(s)$.

Depending on the state the authors distinguish between two different types of space states: Discrete and Continuous.

The Q-values of the quantum agent are computed as the expectation values of a PQC that is fed a state s according to equation 15.

$$Q(s,a) = \langle 0^{\otimes n}|U_\theta^\dagger(s)O_a U_\theta(s)|0^{\otimes n}\rangle \tag{15}$$

where O_a is an observable and n the number of qubits, and the model outputs a vector including Q-values for each possible O_a.

In [9], the authors demonstrate the out-of-distribution generalization for the task of learning in QML, where the training and testing data are drawn from a different distribution. The authors consider the QML task of learning an unknown n-qubit unitary $U \in \mathcal{U}(\mathbb{C}^{2^n})$. The goal is to use training states to optimize the classical parameters α of $V(\alpha)$, an n-qubit unitary QNN, such that for the optimized parameters $\alpha_{opt}, V(\alpha_{opt})$ well predicts the action of U on previously unseen test states. The prediction performance of the trained QNN $V(\alpha_{opt})$ can be quantified in terms of the average distance between the output state predicted by $V(\alpha_{opt})$ and the true output state determined by U.

They provide numerical evidence to support analytical results showing that out-of-distribution generalization is possible for the learning of quantum dynamics. They focused on the task of learning the parameters of an unknown target Hamiltonian by studying the evolution of product states under it. The authors work establishes that for learning unitaries, QNNs trained on quantum data enjoy out-of-distribution generalization between some physically relevant distributions if the training data size is roughly the number of trainable gates.

In [3], the authors propose a new strategy for reducing the number of measurements in variational quantum-classical algorithms (VQCAs) needed for convergence. VQCAs efficiently evaluate a cost function on a QC while optimizing the cost value using a classical computer. Certain issues arise in VQCAs that are not common in classical algorithms, implying that standard off-the-shelf classical optimizers may not be best suited to VQCAs. For example, multiple runs of quantum circuits are required to reduce the effects of shot noise on cost evaluation. An additional complication is that quantum hardware noise flattens the training landscape.

The authors have recently investigated shot-frugal gradient descent for VQCAs, introduced an optimizer, called iCANS (individual Coupled Adaptive Number of Shots), which outperformed off-the-shelf classical optimizers such as Adam for variational quantum compiling and Variational Quantum Eigensolver (VQE) tasks. The key feature of iCANS is that it maximizes the expected gain per shot by frugally adapting the shot noise for each individual partial derivative. In VQE and other VQCAs, it is common to express the cost function $C = \langle H \rangle$ as the expectation value of a Hamiltonian H that is expanded as a weighted sum of directly measurable operators $\{h_i\}_i$ according to equation 16.

$$H = \sum_{i=1}^{N} c_i h_i \tag{16}$$

then C is computed from estimations of each expectation $\langle h_i \rangle$, which is obtained from many shots. The authors proposal is to randomly assign shots to the h_i operators according to a weighted probability distribution proportional to $|c_i|$, they prove that this leads to an unbiased estimator of the cost C, even when the number of shots is extremely small like a single shot. This allows one to unlock a level of shot-frugality for unbiased estimation that simply cannot be accessed without operator sampling. In addition, the randomness associated with operator sampling can provide a means to escape from local minima of C.

A combination of the new sampling strategy with iCANS leads to the main result, which is an improved optimizer for VQCAs that they call Rosalin (Random Operator Sampling for Adaptive Learning with Individual Number of shots). Rosalin retains the crucial feature of maximizing the expected gain per shot. the authors analyze the potential of Rosalin by applying it to VQE for three molecules, namely H_2, LiH, and BeH_2, and compare its performance with that of other optimizers. In cases with more than a few terms in the Hamiltonian, Rosalin outperforms all other optimizer and sampling strategy combinations considered.

In [15], the authors generalise a quantum natural gradient to consider arbitrary quantum states to significantly outperform other VQAs. Quantum Fisher information in the context of general VQCs is a measure that quantifies how much and in what way changing parameters in a quantum circuit affects the underlying quantum state.

The aim of the authors is to minimise the expectation value $E(\underline{\theta}) = Tr[\rho(\underline{\theta})\mathcal{H}]$ of a Hermitian observable $\mathcal{H}$ over the parameters $\underline{\theta}$ using a VQC that depends on these parameters, this circuit produces the quantum states

$\rho(\underline{\theta}) = \Phi(\underline{\theta})\rho_0$ via mapping, and might involve non-unitary transformations due to experimental imperfections or indeed intentional non-unitary elements, such as measurements.

The authors propose a natural gradient update rule, where the quantum Fisher information matrix F_q corrects the gradient vector g_k to account for the dependent and non-uniform effect of the parameters on an arbitrary quantum state $\rho(\underline{\theta})$ mixed or pure. their method also applies to infinite-dimensional quantum states as continuous-variable systems.

The natural gradient descent proposed by the authors in principle allows for improvements relative to imaginary time evolution and the pure-state variant of natural gradient. First even when the objective function is generated by an observable as $E(\underline{\theta}) = Tr[\rho(\underline{\theta})\mathcal{H}]$, their approach allows for general non-unitary elements as Completely Positive Trace-Preserving (CPTP) maps which in principle enable the manipulation of exponentially more degrees of freedom. Second the expected value $E(\underline{\theta}) := Tr[\rho(\underline{\theta})\mathcal{H}]$ is a mapping that is linear in quantum state, their results shown that are well-defined for more general objective functions and its convergence is guaranteed even in the presence of shot noise. When compared to previous studies, the new approach has the advantage that it explicitly takes into account imperfections of the VQC.

In [12], the authors provide an accessible introduction to Quantum Embedding Kernels (QEKs) and then analyze the practical issues arising when realizing them on a noisy near-term QC. QEKs are a subclass of quantum kernel methods where a PQC is used to embed datapoints into the Hilbert space of quantum states. QEKs have certain appealing properties that make them attractive for use, like they limited depth does not require long coherence times, another strong point is that noisy PQCs still lead to well-defined QEKs. The authors propose a series of improvements. First, to use the kernel-target alignment as a cost function to train parameters of the QEK to increase its performance on particular datasets. Second, they propose a mitigation strategy tailored for the QEKs that exploits the kernel's definition to infer the underlying noise levels. Lastly, they propose a strategy for alleviate the influence of noise on the kernel matrix based on a semi-definite program.

The QEK is defined as the inner product between quantum states, which is given by the overlap shown in equation 17.

$$k(\mathrm{x}, \mathrm{x'}) = |\langle\phi(\mathrm{x'})|\phi(\mathrm{x})\rangle|^2 \tag{17}$$

Associated to the quantum feature map $|\phi(\mathrm{x})\rangle$, but we are not able to avoid noise, which means that we cannot assume that the embedded quantum state is pure, then the quantum embedding is realized by a data-dependent density matrix $\rho(\mathrm{x})$ which for pure states reduces to $\rho(\mathrm{x}) = |\phi(\mathrm{x})\rangle\langle\phi(\mathrm{x})|$, with this modification the inner product is given by equation 18.

$$k(\mathrm{x}, \mathrm{x'}) = Tr\{\rho(\mathrm{x})\rho(\mathrm{x'})\} \tag{18}$$

This inner product is also know as the Hilbert-Schmidt inner product for matrices. In summary, any quantum feature map induces a QEK. We can use this kernel as a subroutine in a classical kernel method, for example the Support Vector Machine (SVM), which yields a hybrid quantum-classical approach.

To be able to use QEKs in this way, is needed to evaluate the overlap of two quantum states on near-term hardware. There are a number of advanced algorithms to estimate the overlap of two quantum states. All these algorithms work for arbitrary states, and so they are agnostic to how the states were obtained by necessity. By exploiting the structure and specifics of QEKs, though. The authors propose a better ways to do this overlap, for unitary quantum embeddings they construct the adjoint of the data-encoding circuit $U^\dagger(\mathrm{x})$. Another approach proposed is the SWAP test, based on the SWAP trick, a mathematical gimmick that allow to transform the product of the density matrices into a tensor product [42].

Finally the authors have performed various numerical experiments that showed improvement in classification accuracy after training. They have also investigated noise mitigation techniques and proposed device noise mitigation techniques specific for kernel matrices and combined them with regularization methods. Lastly they tested a large set of combinations, both on simulated depolarizing noise as well as on data from a real quantum processing unit.

C. Comparative analysis of the latest advances

Table I shows the advantage (column "Comparative advantage") of the contribution made (2nd column) by the reference in column "Ref".

D. Bibliographic Discussion

From the literature about the problems and the context of development of the search, it has been possible to delve into the new contributions and their functionalities.

We have noticed that in the QML field, researchers opted for different algorithms competing against each other to see which one gives the best results, QNNs vs. QVAs vs. QKs, each one with its own pros and cons. It will be necessary to observe how these algorithms evolve with the passage of time and the advancement of technology.

E. State of the Art Timeline

Table II shows a timeline of quantum computing major advances.

TABLE I
Comparative Table

Ref	Contribution made	Comparative advantage
[25]	New training method for PQCs that can be used to solve Reinforcement learning tasks for discrete and continuous states spaces based on the deep Q-learning algorithm	Training method for discrete and continuous state spaces for quantum circuits
[9]	Demonstration the Out-of-Distribution generalization for the task of learning in QML where the training and testing data are drawn from different distributions	Ability to extrapolate from training data to unseen data with the potential of QML methods to outperform classical ML
[3]	New strategy for reducing the number of measurements with an adaptive optimizer to construct an improved optimizer called Rosalin that implements stochastic gradient descent while adapting the shot noise for each partial derivative and randomly assigning the shots according to a weighted distribution	Rosalin outperforms other optimizers in the task to find the ground states of molecules H_2, LiH, and BeH_2 without and with quantum hardware noise
[15]	Generalization of quantum natural gradient to consider arbitrary quantum states via completely positive maps, thus the circuits can incorporate both imperfect unitary gates and fundamentally non-unitary operations such as measurements	Demonstration in numerical simulations of noisy quantum circuits the practicality of the new approach and confirm it can significantly outperform other variational techniques
[12]	An accessible introduction to quantum embedding kernels, a analysis of the practical issues arising when realizing them on a noisy near-term QC, and a strategy to mitigate these detrimental effects which is tailored to quantum embedding kernels	Improvement in classification accuracy after training, noise mitigation techniques and regularization methods for specific kernel matrices
[14]	Propose of AES algorithm for Quantum Computing with improved Security using QRW	Propose of Quantum version of AES algorithm with improvement against Quantum attacks
[26]	Explication of QKD and experiments with Quantum Noise	State of art about QKD and experiments with eavesdropper
[7]	Propose parameters and changes to RSA,on QC, to make feasible in actual	Proposes a GEECM, faster algorithm than Shor and experiments with eavesdropper
[28]	Give an overview of QC related to Cybersecurity presenting several Quantum solutions and show how can be used in future to make the area better than now	Proposes a state of art of Quantum attacks, and existing Quantum-based approaches for Cybersecurity

TABLE II
Timeline of Quantum Computing Major Advances

Date	Quantum Computing Major Advances
1970	James Park articulates the no-cloning theorem [17]
1973	Alexander Holevo articulates the Holevo's Theorem and Charles H. Bennet shows that computation can be done reversibly [6]
1980	Paul Beinoff describes the 1st quantum mechanical computer model [5], Tomasso Toffoli introduces the Toffoli Gate [27]
1985	David Deutsch describes the 1st universal QC
1992	David Deutsch and Richard Jozsa propose a computational problem that can be solved efficiently with the Deutsch–Jozsa algorithm on a QC
1993	Dan Simon invents an oracle problem, for which a QC would be exponentially faster than a conventional computer
1994	Peter Shor publishes the Shor's Algorithm
1995	Peter Shor proposes the 1st schemes for quantum error correction [24]
1996	Lov Grover invents the quantum DB search algorithm
2000	Arun K. Pati and Samuel L. Braunstein proved the quantum no-deleting theorem
2001	First execution of Shor's algorithm
2003	Implementation of the Deutsch–Jozsa algorithm on a QC
2006	First 12 qubit QC benchmarked
2007	D-Wave Systems demonstrates use of a 28-qubit annealing QC
2009	First electronic quantum processor created
2010	Single-electron qubit developed
2014	Scientists transfer data by quantum teleportation over a distance of 3 m with 0% error rate [19]
2017	IBM unveils 17-qubit QC
2018	Google announces the creation of a 72-qubit quantum chip
2019	IBM reveals its biggest QC yet, consisting of 53 qubits
2020	Google engineers report the largest chemical simulation on a QC
2021	IBM claims that it has created a new 127 quantum bit processor
2022	Researchers at Google Quantum AI Team Make Traversable Wormhole with a QC
2023	Researchers of Innsbruck have entangled two ions over a distance of 230 m

F. Expected or surprising results

While we look for information for this survey, we read a diversity of articles, where some of them appears to be science fiction or coming out from a movie, but they are real scientific investigations like [13] in Nature. This article caused some controversy and what we least want is to get into controversy, but we must not forget that it is an amazing experiment and discovery.

Another point that caught the attention is the rapid advance of quantum computing. It is a subject that is not heard as much as AI or neural networks, but it is a field that is advancing by leaps and bounds. So we are happy to contribute with this survey.

IV. Conclusions

Quantum Computing is still in its early stages, and building a functional and efficient QC with enough qubits will take years.

QCs have the ability to simulate molecular behavior at a fundamental level, making them valuable for various industries. Automakers like Volkswagen and Daimler use

QCs to analyze and improve the composition of electric vehicle batteries. Pharmaceutical companies also utilize QCs to study chemicals and explore new possibilities for medicine development. Quantum computing has the potential to revolutionize society, with its ability to solve optimization problems quickly by evaluating numerous solutions. Airbus employs QCs to determine fuel-efficient flight paths, while Volkswagen has developed a tool for optimizing bus and taxi routes to reduce traffic congestion. Some scientists believe that QCs could accelerate advancements in AI. However, the full extent of quantum computing's potential may take many years to realize.

The QML domain should also target designing new quantum learning models that will observe patterns under quantum mechanics schemes, not classical statistical theory. This will provide an opportunity to explore new model architectures that might overcome classical machine learning limitations.

The development of post-quantum cryptography is crucial to mitigate the cybersecurity risks posed by quantum computing. Post-quantum cryptography refers to algorithms that are resistant to attacks from QCs. It not only improves database search capabilities but also addresses optimization problems in various business domains such as data analytics, logistics, and medical research.

Discovering better algorithms to work with quantum computing is still an open area of research. Finally, this study gives an overview of QML, quantum cybersecurity and recent studies in quantum computations with its possible applications.

References

[1] Feynman, R. P. (1982). Simulating physics with computers. Int. J. Theor. Phys. 21, 467–488

[2] Díaz, A., Rodriguez, M., Piattini, M. (2024): Towards a set of metrics for hybrid (quantum/classical) systems maintainability. Journal of Universal Computer Science, vol. 30, no. 1, pp. 25-48

[3] Arrasmith, A., Cincio, L., Somma, R. D., Coles, P. J. (2020). Operator sampling for shot-frugal optimization in variational algorithms.

[4] Bausch, J. (2020). Recurrent Quantum Neural Networks. Advances in Neural Information Processing Systems, (Eds.) H. Larochelle, M. Ranzato, R. Hadsell, M.F. Balcan, H. Lin, Vol. 33, pp. 1368–1379, Curran Associates, Inc., https://proceedings.neurips.cc/papers/search?q=quantum

[5] Benioff, P. (1980, May). The computer as a physical system: A microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines. Journal of Statistical Physics, 22(5), 563-591. doi:10.1007/BF01011339

[6] Bennett, C. H. (1973). Logical reversibility of computation. IBM Journal of Research and Development, 17(6), 525-532. doi:10.1147/rd.176.0525

[7] Bernstein, D. J., Heninger, N., Lou, P., Valenta, L. (2017). Post-quantum rsa. Cryptology ePrint Archive, Paper 2017/351. https://eprint.iacr.org/2017/351

[8] Brooks, M. (2019, October). Beyond quantum supremacy: the hunt for useful quantum computers. Nature, 574(7776), 19-21. doi:10.1038/d41586-019-02936-3

[9] Caro, M. C., Huang, H.-Y., Ezzell, N., Gibbs, J., Sornborger, A. T., Cincio, L.,. . . Holmes, Z. (2022). Out-of-distribution generalization for learning quantum dynamics.

[10] Cerezo, M., Arrasmith, A., Babbush, R., Benjamin, S. C., Endo, S., Fujii, K., ... Coles, P. J. (2021, aug). Variational quantum algorithms. Nature Reviews Physics, 3(9), 625–644. doi:10.1038/s42254-021-00348-9

[11] Cong, I., Choi, S., Lukin, M. D. (2019, aug). Quantum convolutional neural networks. Nature Physics, 15(12), 1273–1278. doi:10.1038/s41567-019-0648-8

[12] Hubregtsen, T., Wierichs, D., Gil-Fuster, E., Derks, P.-J. H. S., Faehrmann, P. K., Meyer, J. J. (2022, oct). Training quantum embedding kernels on near-term quantum computers. Physical Review A, 106 (4). doi:10.1103/physreva.106.042431

[13] Jafferis, D., Zlokapa, A., Lykken, J. D., Kolchmeyer, D. K., Davis, S. I., Lauk, N., . . . Spiropulu, M. (2022, Dec 01). Traversable wormhole dynamics on a quantum processor. Nature, 612(7938), 51-55. doi:10.1038/s41586-022-05424-3

[14] Ko, K.-K., Jung, E.-S. (2021). Development of cybersecurity technology and algorithm based on quantum computing. Applied Sciences, 11(19). doi:10.3390/app11199085

[15] Koczor, B., Benjamin, S. C. (2022). Quantum natural gradient generalised to noisy and non-unitary circuits.

[16] Otterbach, J. S., Manenti, R., Alidoust, N., Bestwick, A., Block, M., Bloom, B., ... Rigetti, C. (2017). Unsupervised machine learning on a hybrid quantum computer.

[17] Park, J. L. (1970). The concept of transition in quantum mechanics. Foundations of Physics, 1, 23-33.

[18] Peruzzo, A., McClean, J., Shadbolt, P., Yung, M.-H., Zhou, X.-Q., Love, P. J., ... O'Brien, J. L. (2014, jul). A variational eigenvalue solver on a photonic quantum processor. Nature Communications, 5(1). doi:10.1038/ncomms5213

[19] Pfaff, W., Hensen, B. J., Bernien, H., van Dam, S. B., Blok, M. S., Taminiau, T. H., . . . Hanson, R. (2014, aug). Unconditional quantum teleportation between distant solid-state quantum bits. Science, 345(6196), 532–535. doi:10.1126/ science.1253512

[20] Preskill, J. (2018, August). Quantum Computing in the NISQ era and beyond. Quantum, 2, 79. doi:10.22331/q-2018-08-06-79

[21] Raussendorf, R. (2012). Key ideas in quantum error correction. Philo- sophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences , 370 (1975), 4541-4565. doi:10.1098/rsta.2011.0494

[22] S, N., Singh, H., N, A. U. (2022). An extensive review on quantum computers. Advances in Engineering Software, 174, 103337. https://doi.org/10.1016/j.advengsoft.2022.103337

[23] Schuld, M. (2021). Supervised quantum machine learning models are kernel methods.

[24] Shor, P. W. (1995, October). Scheme for reducing decoherence in quantum computer memory, 52(4), R2493-R2496. doi:10.1103/PhysRevA.52.R2493

[25] Skolik, A., Jerbi, S., Dunjko, V. (2022, may). Quantum agents in the gym: a variational quantum algorithm for deep q-learning. Quantum, 6, 720. doi:10.22331/q-2022-05-24-720

[26] Tianqi Zhou, X. L., Jian Shen. (2018). Quantum cryptography for the future internet and the security analysis. Security and Communication Networks. https://doi.org/10.1155/2018/8214619

[27] Toffoli, T. (1980). Reversible computing. In J. de Bakker J. van Leeuwen (Eds.), Automata, languages and programming (pp. 632–644). Berlin, Heidelberg: Springer Berlin Heidelberg.

[28] Uttam Ghosh, P. C., Debashis Das. (2023). A comprenhensive tutorial on cybersecurity in quantum computing paradigm. TechRxiv. https://doi.org/10.36227/techrxiv.22277251.v1

[29] Wecker, D., Hastings, M. B., Troyer, M. (2015, oct). Progress towards practical quantum variational algorithms. Physical Review A, 92(4). doi:10.1103/physreva.92.042303

[30] Whitfield, J. D., Yang, J., Wang, W., Heath, J. T., Harrison, B. (2022). Quantum computing 2022.

[31] Pogorelov, I. and Feldker, T. and Marciniak, Ch. D. and Postler, L. and Jacob, G. and Krieglsteiner, O. and Podlesnic, V. and Meth, M. and Negnevitsky, V. and Stadler, M. and Höfer, B. and Wächter, C. and Lakhmanskiy, K. and Blatt, R. and Schindler, P. and Monz, T. (2021): Compact Ion-Trap Quantum Computing Demonstrator. PRX Quantum, vol. 2, 2, pp. 020343, https://link.aps.org/doi/10.1103/PRXQuantum.2.020343

[32] Sangil Kwon, Akiyoshi Tomonaga, Gopika Lakshmi Bhai, Simon J. Devitt, Jaw-Shen Tsai (2021): Gate-based supercon-

ducting quantum computing. J. Appl. Phys. 129(4): 041102. https://doi.org/10.1063/5.0029735
[33] June Sang Lee, Nikolaos Farmakidis, C. David Wright and Harish Bhaskaran (2022): Polarization-selective reconfigurability in hybridized-active-dielectric nanowires. Science Advances, 8 eabn9459. DOI:10.1126/sciadv.abn9459
[34] Wurtz, J. et al. (2023): Aquila: Quera's 256-qubit neutral-atom quantum computer. https://arxiv.org/abs/2306.11727.
[35] Kornjača, M., Samajdar, R., Macrì, T. et al. (2023): Trimer quantum spin liquid in a honeycomb array of Rydberg atoms. Commun Phys 6, 358 (2023). https://doi.org/10.1038/s42005-023-01470-z
[36] Steven H. Adachi, Maxwell P. Henderson (2015): Application of Quantum Annealing to Training of Deep Neural Networks. arXiv:1510.06356 https://arxiv.org/abs/1510.06356
[37] Cao, Yudong, Romero, Jonathan, Olson, Jonathan P., Degroote, Matthias, Johnson, Peter D., Kieferová, Mária, Kivlichan, Ian D., Menke, Tim, Peropadre, Borja, Sawaya, Nicolas P.D., Sim, Sukin, Veis, Libor, Aspuru-Guzik, Alán (2019): Quantum Chemistry in the Age of Quantum Computing. Chemical Reviews, Vol. 119, No. 19, pp. 10856–10915, https://doi.org/10.1021/acs.chemrev.8b00803
[38] Ma, H., Govoni, M. Galli, G. (2020): Quantum simulations of materials on near-term quantum computers. npj Comput Mater 6, 85. https://doi.org/10.1038/s41524-020-00353-z
[39] Sivarajah, Ilamaran. (2022): What is Quantum Control Theory?. AZoQuantum. Retrieved on March 06, 2024 from https://www.azoquantum.com/Article.aspx?ArticleID=335
[40] Riccardo Bassoli, Holger Boche, Christian Deppe, Roberto Ferrara, Frank H. P. Fitzek, Gisbert Janssen, Sajad Saeedinaeeni (2021): Quantum Communication Networks. Foundations in Signal Processing, Communications and Networking. Springer. https://doi.org/10.1007/978-3-030-62938-0
[41] Len, Y.L., Gefen, T., Retzker, A. et al. (2022): Quantum metrology with imperfect measurements. Nat Commun 13, 6971. https://doi.org/10.1038/s41467-022-33563-8
[42] Harry Buhrman, Richard Cleve, John Watrous, Ronald de Wolf (2001). Quantum Fingerprinting. Physical Review Letters. 87 (16): 167902. doi:10.1103/PhysRevLett.87.167902