UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

A Review on Quantum Machine Learning and Quantum Cryptography

Felipe Cisternas Álvarez
Jean-Pierre Villacura
Universidad Técnica Federico Santa María, Chile

Valparaíso, 2024

UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

Content

- Introduction
- Brief overview of Quantum Computing
- State of the Art
- Conclusions

UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

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

This paper explores a range of subjects concerning quantum computing, including quantum computers and technologies.

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.

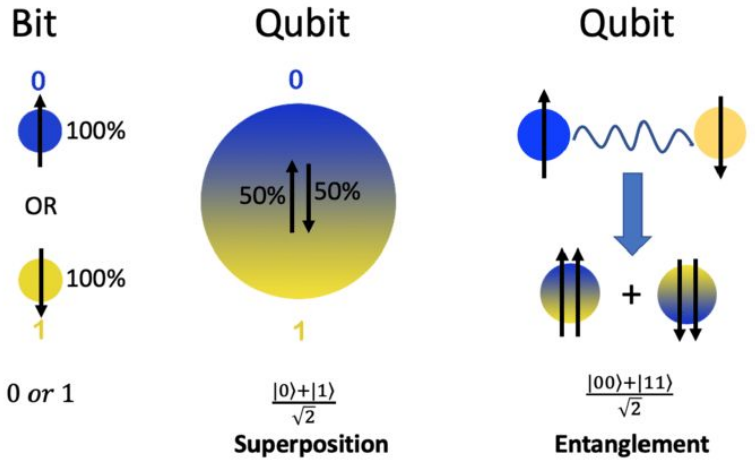
UNIVERSIDAD TECNICA FEDERICO SANTA MARIA

Brief overview of Quantum Computing

Quantum Computing

Three main Principles:

- **Superposition**
- **Entanglement**
- **Decoherence**



The Current state of Quantum Computing is referred to as the "Noisy Intermediate-Scale Quantum" (NISQ)

UNIVERSIDAD TECNICA FEDERICO SANTA MARIA

Brief overview of Quantum Computing

QCs and Technologies:

- Gate-Based Ion Trap Processors
- Gate-Based Superconducting Processors
- Photonic Processors
- Neutral Atom Processors
- Rydeberg Atom Processors
- Quantum Annealers

Qubit Type	Pros/Cons	Select Players
Superconducting	***Pros***: High gate speeds and fidelities. Can leverage standard lithographic processes. Among first qubit modalities so has a head start. ***Cons***: Requires cryogenic cooling; short coherence times; microwave interconnect frequencies still not well understood.	rigetti, Google, IBM Q, QuTech, OQC, IQM, Quantum Circuits, Inc, 本源量子 Origin Quantum
Trapped Ions	***Pros***: Extremely high gate fidelities and long coherence times. Extreme cryogenic cooling not required. Ions are perfect and consistent. ***Cons***: Slow gate times/ operations and low connectivity between qubits. Lasers hard to align and scale. Ultra-high vacuum required. Ion charges may restrict scalability.	IONQ, AQT, QUANTINUUM, oxford ionics, Universal Quantum
Photonics	***Pros***: Extremely fast gate speeds and promising fidelities. No cryogenics or vacuums required. Small overall footprint. Can leverage existing CMOS fabs. ***Cons***: Noise from photon loss; each program requires its own chip. Photons don't naturally interact so 2Q gate challenges.	PsiQuantum, XANADU, QUIX QUANTUM, ORCA Computing
Neutral Atoms	***Pros***: Long coherence times. Atoms are perfect and consistent. Strong connectivity, including more than 2Q. External cryogenics not required. ***Cons***: Requires ultra-high vacuums. Laser scaling challenging.	ColdQuanta, QuEra Computing Inc., atom computing, PASQAL
Silicon Spin/Quantum Dots	***Pros***: Leverages existing semiconductor technology. Strong gate fidelities and speeds. ***Cons***: Requires cryogenics. Only a few entangled gates to-date with low coherence times. Interference/cross-talk challenges.	intel, Silicon Quantum Computing, diraq, QUANTUM MOTION, QUANTUM BRILLIANCE

UNIVERSIDAD TECNICA FEDERICO SANTA MARIA

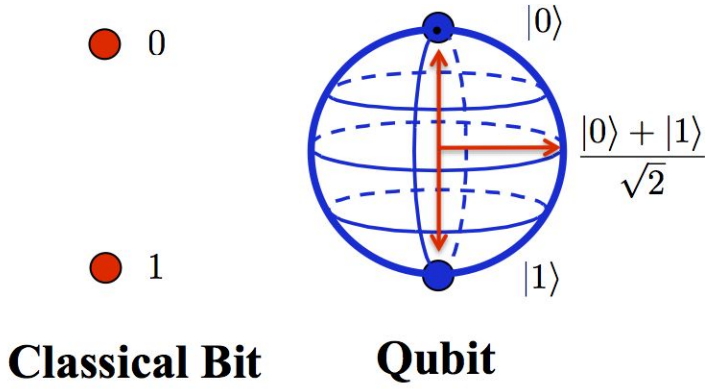
Brief overview of Quantum Computing

Quantum Data:

Is any data source that occurs in natural or artificial quantum systems and exhibits superposition & entanglement, leading to joint probability distributions that could requiere an exponential amount of classical resources to represent or store.

Some examples can be:

- Chemical Simulations
- Quantum Matter Simulations
- Quantum Control
- Quantum Communication Networks
- Quantum Metrology



UNIVERSIDAD TECNICA FEDERICO SANTA MARIA

Brief overview of Quantum Computing

Quantum Gates:

X Gate
Bit–flip, Not

$$X \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \beta|0\rangle + \alpha|1\rangle$$

Z Gate
Phase–flip

$$Z \equiv \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \alpha|0\rangle - \beta|1\rangle$$

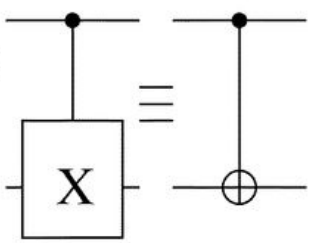
H Gate
Hadamard

$$H \equiv \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \frac{\alpha+\beta|0\rangle + \alpha-\beta|1\rangle}{\sqrt{2}}$$

T Gate

$$T \equiv \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \alpha|0\rangle + e^{i\pi/4}\beta|1\rangle$$

Controlled Not
Controlled X
CNot

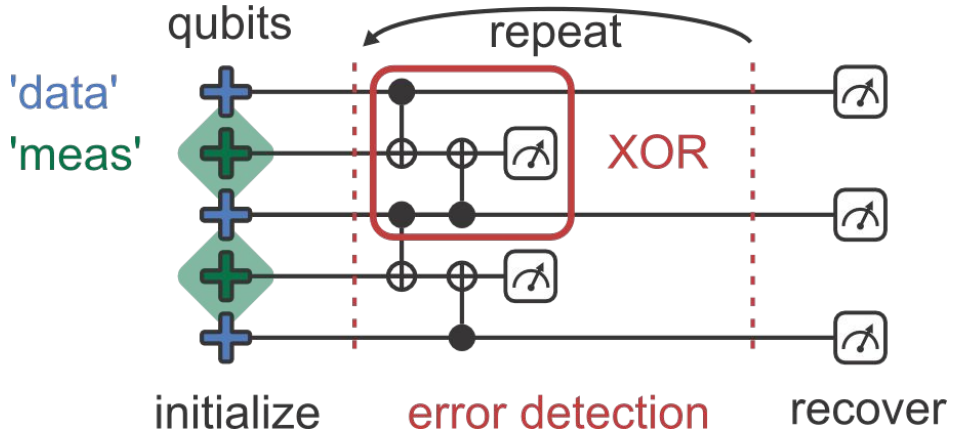


$$\equiv \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} a \\ b \\ c \\ d \end{bmatrix} = \begin{matrix} a|00\rangle + b|01\rangle + \\ d|10\rangle + c|11\rangle \end{matrix}$$

UNIVERSIDAD TECNICA FEDERICO SANTA MARIA

Brief overview of Quantum Computing

- **Noise & Quantum Error Correction (QEC):**
  - **Noise** is present in modern day QCs, Qubits are suceptible to interference from the surrounding enviroment, imperfect fabrication, TLS and sometimes even gamma rays.
  - **QEC** is used in QCs to protect quantum information from errors due to decoherence and other quantum noise, traditional error correction methods employs over repetition.



UNIVERSIDAD TECNICA FEDERICO SANTA MARIA

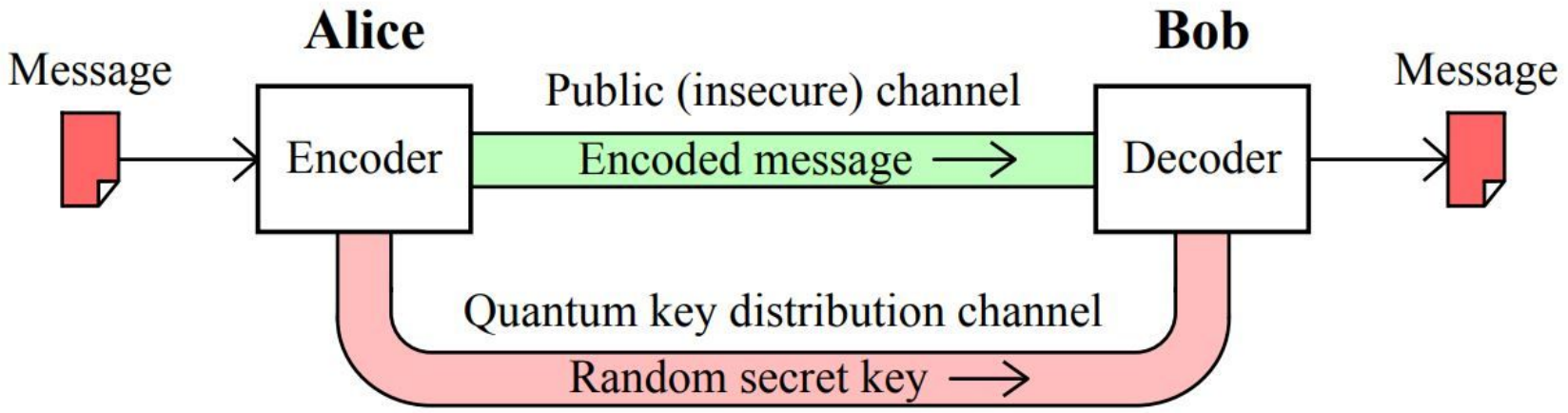
Brief overview of Quantum Computing

Quantum Cybersecurity:

- **Quantum Cryptography**

  "nobody knows exactly when quantum computing will become a reality, but when and if it does, it will signal the end of traditional cryptography". (Boukhonine, 1998).

- **Quantum Key Distribution**



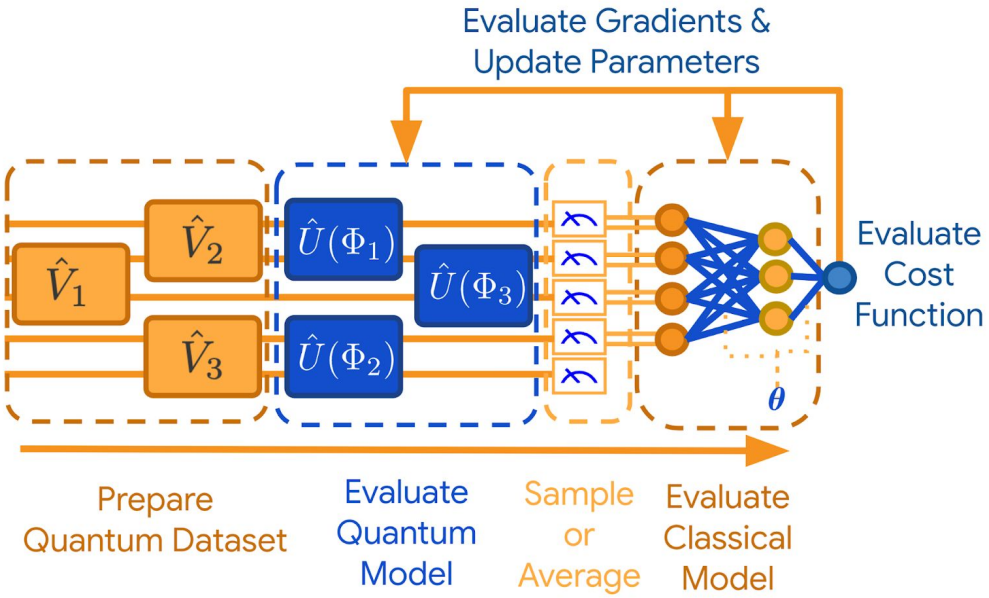
UNIVERSIDAD TECNICA FEDERICO SANTA MARIA

Brief overview of Quantum Computing

Quantum Machine Learning (QML):

QML aims to understand the ultimate limits of data analysis allowed by the laws of physics. Some algorithms being researched are

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



UNIVERSIDAD TECNICA FEDERICO SANTA MARIA

State of the Art

State of the Art Timeline:

Date	Quantum Computing Major Advances
1970	James Park articulates the no-cloning theorem (28)
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 (38)
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 (35)
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 (30)
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

UNIVERSIDAD TECNICA FEDERICO SANTA MARIA

State of the Art

Metodology

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 **Quantum Machine Leanring**, it was used the **Snowball** methodology, reading the citations of the most recent papers on QML.

UNIVERSIDAD TECNICA FEDERICO SANTA MARIA

State of the Art

Quantum Cybersecurity:

- Development of Cybersecurity Technology and Algorithm Based on Quantum Computing [Ko, et al. 2021]

> Advanced Encryption System (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, making it difficult to predict the correct order during the decryption process, achieving greater security than classical approach.

UNIVERSIDAD TECNICA FEDERICO SANTA MARIA

State of the Art

Quantum Cybersecurity:

- Quantum Cryptography for the future internet and security Analysis [Zhou, et al. 2018]

In this work, the authors focus on analyzing characteristics of the quantum cryptography and exploring of the advantages of it in the future internet. They analyze the Quantum Key Distribution protocol in the noise-free channel by making measurements of different variables. Probability of the eavesdropper being detected v/s Number of photones 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.

UNIVERSIDAD TECNICA FEDERICO SANTA MARIA

State of the Art

Quantum Cybersecurity:

- A comprehensive Tutorial on Cybersecurity in Quantum Computing Paradigm [Gosh, et al. 2023]

In this work, the authors make a contribution in the state of art of Cybersecurity from wide perspectives.

They give and 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.

UNIVERSIDAD TECNICA FEDERICO SANTA MARIA

State of the Art

Quantum Cybersecurity:

- Post-Quantum RSA [Bernstein, et al. 2017]

In this work, the authors make a contribution proposing paramethers 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.

Proposes a new Quantum Algorithm to generate factor numbers, GEECM faster than Shor and algorithms of classic paradigm and a new .

UNIVERSIDAD TECNICA FEDERICO SANTA MARIA

State of the Art

Quantum Machine Learning:

- Quantum agents in the Gym: a variational quantum algorithm for deep Q-learning [Skolik, et al. 2022]

The Q-Values of the quantum agent are computed as the expectation values of a PQC that is fed a state s as:

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

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.

UNIVERSIDAD TECNICA FEDERICO SANTA MARIA

State of the Art

Quantum Machine Learning:

- Out-of-distribution generalization for learning quantum dynamics [Caro et al. 2022]

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.

UNIVERSIDAD TECNICA FEDERICO SANTA MARIA

State of the Art

Quantum Machine Learning:

- Operator Sampling for Shot-frugal Optimization in Variational Algorithms [Arrasmith, et al. 2020]

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 $\{h_i\}_i$:

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

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).

UNIVERSIDAD TECNICA FEDERICO SANTA MARIA

State of the Art

Quantum Machine Learning:

- Quantum natural gradient generalised to noisy and non-unitary circuits [Kozcor, et al. 2022]

Quantum Fisher information in the context of general variational quantum circuits 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 variational quantum circuit 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.

UNIVERSIDAD TECNICA FEDERICO SANTA MARIA

State of the Art

Quantum Machine Learning:

- Training Quantum Embedding Kernels on Near-Term Quantum Computers [Hubregtsen, et al. 2022]

The quantum embedding kernel is defined as the inner product between quantum states, which is given by the overlap

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

Associated to the quantum feature map $|\phi(\mathbf{x})\rangle$, 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 $\rho(\mathbf{x})$ which for pure states reduces to $\rho(\mathbf{x}) = |\phi(\mathbf{x})\rangle\langle\phi(\mathbf{x})|$, with this modification the inner product is given by

$$k(\mathbf{x}, \mathbf{x'}) = Tr\{\rho(\mathbf{x})\rho(\mathbf{x'})\}$$

UNIVERSIDAD TECNICA FEDERICO SANTA MARIA

State of the Art

Authors	contribution made	Comparative advantage
Andrea Skolik Sofiene Jerbi Vedran Dunjko	New training method for PQCs that can be used to solve Reinforcement learning tasks for discrete and continousstates spaces based on the deep Q-learning algorithm	Training method for discrete and continous state spaces for quantum circuits
Mathias Caro Hsin-Yuan Huang Nicholas Ezzel Joe Gibbs Andrew Sornborger Lukasz Cincio Patrick Coles Zoe Holmes	Demonstration the Out-of-Distribution generalization, for the task of learning in Quantum Machine learning where the training and testing data are drawn from differents distributions	Ability to extrapolate from training data to unseen data with the potential of Quantum Machine Learning methods tooutperform clasical Machine Learning
Andrew Arrasmith Lukasz Cincio Rolando Somma Patrick Coles	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
Bálint Kozcor Simon Benjamin	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.
Thomas Hubregtsen David Wierichs Elies Gil-Fuster Peter-Jan Dereks Paul Faehrmann Johannes Meyer	An accessible introduction to quantum embedding kernels, a analysis of the practical issues arising when realizing them on a noisy near-term quantum computer, 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.
Kyung-Kyu Ko Eun-SUng Jung	Propose of AES Algorithm for Quantum Computing with improved Security using Quantum Random Walk.	Propose of Quantum version of AES algorithm with improvement against Quantum attacks
Tianqi Zhou Jian Shen Xiong Li	Explication of Quantum Key Distribution and experiments with Quantum Noise	State of art about Quantum Key Distribution and experiments with eavesdropper
Daniel Bernstein Nadia Heninger	Propose paramethers and changes to RSA, on Quantum Computing, to make feasible in actual.	Proposes a GEECM, faster algorithm than Shor and experiments with eavesdropper
Utham Ghosh Debashi Das Pushpita Shatterje	Give an overview of quantum computing 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 approeaches for Cybersecurity.

UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

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.

The QML domain should also target designing new quantum learning models that will observe patterns under quantum mechanics schemes, not classical statistical theory.

The development of post-quantum cryptography is crucial to mitigate the cybersecurity risks posed by quantum computing

Thanks for your attention.