

# Quantum Circuits as Novel Activation Functions in Cryptography

Javier Orduz<sup>1,2,3</sup>, Nagaraj<sup>1</sup>

<sup>1</sup>EC, Qmexico<sup>2</sup>

<sup>13</sup>Quaker-ECE

March 17, 2025

## 4 QC &amp; AI

# Conceptual framework

QC & AI

Javier  
Orduz<sup>1,2,3</sup>,  
Nagaraj<sup>1</sup>

Contents

Protocols and  
methods for  
encryption

Applications

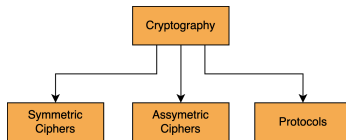
QC & AI

References

## Definition 1 (Cryptography)

Literature shows different definitions, and some of these are [2]

- The discipline that embodies the principles, means, and methods for transforming data to encrypt semantic content, prevent unauthorized use or undetected modification .
- It is the science of encrypting information to conceal its content .



# Conceptual framework

QC & AI

Javier  
Orduz<sup>1,2,3</sup>,  
Nagaraj<sup>1</sup>

Contents

Protocols and  
methods for  
encryption

Applications

QC & AI

References

## Definition 2 (Shannon Entropy)

It is given by

$$S = - \sum_{i=1}^k p_i \log_2 p_i \quad (1)$$

The entropy of uncertainty of a random variable  $X$  with probabilities  $p_1, \dots, p_n$ .

## Definition 3 (Von Neumann Entropy)

In the quantum information context,

$$H_V = - \sum_{i=1}^n \lambda_i \log_2 \lambda_i \quad (2)$$

Where  $\lambda_i$  are the eigenvalues of a density operator .

# (some) Concepts

QC & AI

Javier  
Orduz<sup>1,2,3</sup>,  
Nagaraj<sup>1</sup>

Contents

Protocols and  
methods for  
encryption

Applications

QC & AI

References

## Definition 4 (Trapdoor function, trapdoor one-way function )

A function  $f : \{0, 1\}^* \rightarrow \{0, 1\}^*$  is called **one-way** if the following two conditions hold . We additionally have the following two definitions,

1. A function that is simple to compute but difficult to invert without additional information is known as a **trapdoor function** .
2. A function that is easy to compute, but whose inverse is computationally infeasible to determine without specific privileged information.

## Definition 5 (Protocol)

A **set of rules** used by two or more communicating entities that describe the message order and data structures for information exchanged between the entities is called **protocol** .

## Definition 6 (One-Time-Pad protocol)

The protocol encrypts a message using a public channel and uses the XOR operation.

# Implementation: QC and ML

QC & AI

Javier  
Orduz<sup>1,2,3</sup>,  
Nagaraj<sup>1</sup>

Contents

Protocols and  
methods for  
encryption

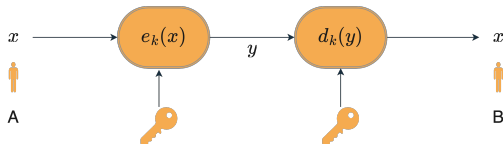
Applications

QC & AI

References

We use  $B$  the text in binary is  $H = 1001000_2 = 72_{10}$  and ciphertext in binary system is  $Z = 1011010_2 = 90_{10}$ . The subscripts refer to binary and decimal systems. We notice that

$$\begin{aligned} B = DEC(C, K) &= DEC(ENC(B, K), K) \\ &= DEC(B \oplus K, K) \\ &= B \oplus K \oplus K \\ &= B \end{aligned} \tag{3}$$



# Example

QC & AI

Javier  
Orduz<sup>1,2,3</sup>,  
Nagaraj<sup>1</sup>,

Contents

Protocols and  
methods for  
encryption

Applications

QC & AI

References

1. Encryption: To obtain ciphertext,  $C = ENC(B, K) = B \oplus K$
2. Decryption: To retrieve the original text,  $B = DEC(C, K) = C \oplus K$

Example

1. Encryption.

$$\begin{array}{rcl} 1001000 & \rightarrow & H \\ \oplus 0010010 & \rightarrow & 18 \\ \hline 1011010 & \rightarrow & Z \end{array}$$

2. Decryption

$$\begin{array}{rcl} 1011010 & \rightarrow & Z \\ \oplus 0010010 & \rightarrow & 18 \\ \hline 1001000 & \rightarrow & H \end{array}$$

# Quantum Concepts

QC & AI

Javier  
Orduz<sup>1,2,3</sup>,  
Nagaraj<sup>1</sup>

Contents

Protocols and  
methods for  
encryption

Applications

QC & AI

References

## Definition 7 (Quantum key exchange (QKE))

It is the idea of leveraging quantum mechanics to improve classical protocols.

## Definition 8 (BB84 protocol)

Let A and B, two individuals, exchange information using two points. Person A employs two distinct orthogonal bases to transmit the data.

## Definition 9 (B92 protocol)

This protocol implements one non-orthogonal basis to send information.



# Applications

QC & AI

Javier  
Orduz<sup>1,2,3</sup>,  
Nagaraj<sup>1</sup>

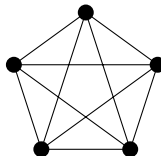
Contents

Protocols and  
methods for  
encryption

Applications

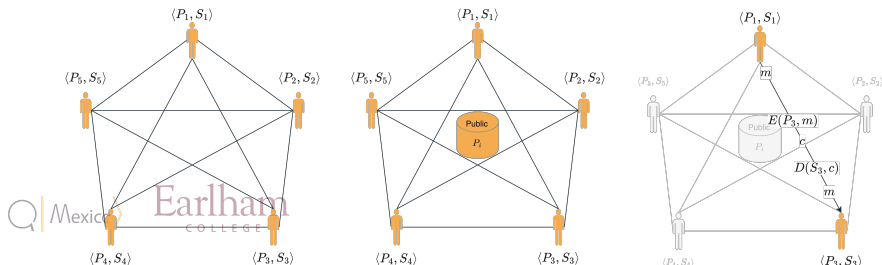
QC & AI

References



**Figure:** Graph for  $n = 5$  and  $k = 2$ : This represents a network with  $n = 5$  users, where  $k = 2$  users are engaged in pairwise communication.

- We will swap points and
- edges



## Definition 10 (Activation Functions)

Nonlinear functions that send a weighted sum of the inputs to a node.

Examples: Sigmoid, ReLU, softplus,  $\tanh x$

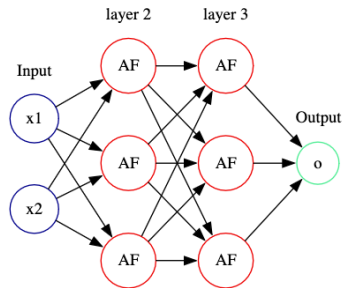
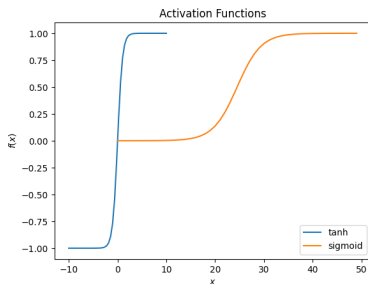


Figure: Examples of Activation functions and a fully connected network.

# Neural Networks for Cryptography

QC & AI

Javier  
Orduz<sup>1,2,3</sup>,  
Nagaraj<sup>1</sup>

Contents

Protocols and  
methods for  
encryption

Applications

QC & AI

References

## Theorem 11 (Cybenko)

*Let  $f : \mathbb{R}^d \rightarrow \mathbb{R}$  be a function<sup>1</sup> on a compact set  $K \subset \mathbb{R}^d$ . Then for any  $\epsilon > 0$  there exists a neural network with a single hidden layer of the form*

$$\phi(x) = \sum_{i=1}^N \sum_{j=1}^d w_i^{(1)} \sigma(w_{ij}^{(0)} x_j + b_i^{(0)}) + b^{(1)},$$

$\theta = \{w_{ij}^{(0)}, w_i^{(1)}, b_i^{(0)}, b^{(1)}\}$ , where  $\sigma : \mathbb{R} \rightarrow \mathbb{R}$  is an activation function<sup>2</sup>, such that

$$\sup_{x \in K} |f(x) - \phi(x)| < \epsilon.$$

The parameter  $N$  is known as the **width** [1].

<sup>1</sup>continuous

<sup>2</sup>non-polynomial non-linear

# Examples: Activation Function

QC & AI

Javier  
Ordúz<sup>1,2,3</sup>,  
Nagaraj<sup>1</sup>

Contents

Protocols and  
methods for  
encryption

Applications

QC & AI

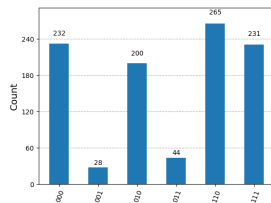
References

$$\sigma(x) = \text{ReLU}(x) = \max(0, x)$$

$$\sigma(x) = \text{sigmoid}(x) = \frac{1}{1 + e^{-x}}$$

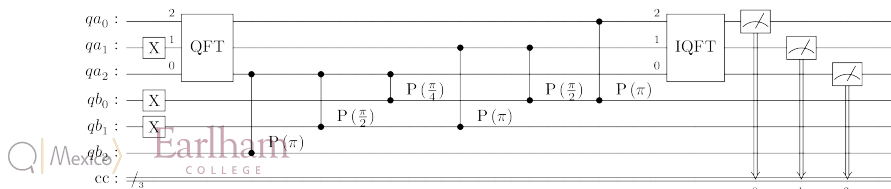
$$\sigma(x) = \tanh x$$

$$\sigma(x) = \cos x, \sin x$$



**Figure:** Addition=2 + 3 operation with QCircuits and simulator.

**Figure:** Webbook: <https://earlham-college.github.io/quaker-ece/>



**Figure:** Partial implementation of AF

# Conclusions and Discussion

QC & AI

Javier  
Orduz<sup>1,2,3</sup>,  
Nagaraj<sup>1</sup>,

Contents

Protocols and  
methods for  
encryption

Applications

QC & AI

References

- This paper explored fundamental concepts in cybersecurity/cryptography and their equivalents in the quantum domain.
- It also provided foundational information on key protocols in both classical and quantum cryptography.
- We replaced the activation function with a quantum circuit and analyzed potential options for security.

# Future directions

QC & AI

Javier  
Orduz<sup>1,2,3</sup>,  
Nagaraj<sup>1</sup>

Contents

Protocols and  
methods for  
encryption

Applications

QC & AI

References

- Future work aims to expand on these fundamental concepts, incorporating emerging ideas from quantum computing, machine learning, and deep learning to contribute to developing next-generation cryptographic methods, particularly in the post-quantum cryptography era.
  - Implement this and more experiments on a real quantum computer.
- Explore and implement other options/circuits.



Figure: Webbook: <https://github.com/jaorduz/QCandAI>

**Thank you!**



# References

QC & AI

Javier  
Orduz<sup>1,2,3</sup>,  
Nagaraj<sup>1</sup>,

Contents

Protocols and  
methods for  
encryption

Applications

QC & AI

References

- [1] Jim Halverson. Tasi lectures on physics for machine learning, 2024.
- [2] Javier Orduz. Mathematical foundations for Modern Cryptography in the Quantum Era. 2025. Accepted to be published soon.



Figure: <https://jaorduz.github.io/files/2025/APSsldsA.pdf>