Foundations For Modern Quantum Cryptography

Javier Orduz

[1]FESAc-UNAM

January 26, 2026

1 Contents

2 Objective

3 Abstract

4 Classical concepts

5 Quantum concepts I

6 Concepts for encryption and a case study

7 Quantum concepts II

8 Toy model

9 Cryptography, QC & AI

10 References

Objective

Objective

To introduce key ideas in cybersecurity and explore how they extend into the quantum world. We present classical and quantum cryptographic approaches and briefly discuss how emerging tools from quantum computing and machine learning are shaping the future of secure systems in the post-quantum era.

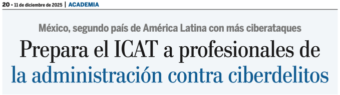
Q|Mexico⟩

qaldas

Abstract

We examine key concepts in cybersecurity and their counterparts in the quantum domain, providing an overview of both classical and quantum cryptographic protocols. This work aims to bridge foundational security principles with emerging quantum technologies.

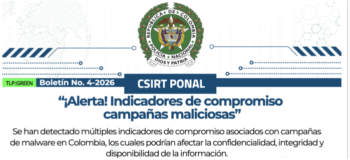
Some domestic and international news



20 • 11 de diciembre de 2025 | ACADEMIA

México, segundo país de América Latina con más ciberataques

Prepara el ICAT a profesionales de la administración contra ciberdelitos

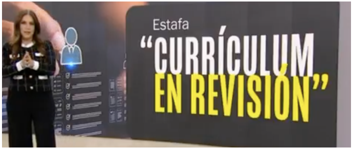


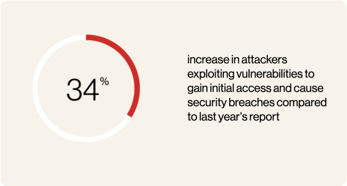
TLP:GREEN Boletín No. 4-2026

CSIRT PONAL

“¡Alerta! Indicadores de compromiso campañas maliciosas”

Se han detectado múltiples indicadores de compromiso asociados con campañas de malware en Colombia, los cuales podrían afectar la confidencialidad, integridad y disponibilidad de la información.





increase in attackers exploiting vulnerabilities to gain initial access and cause security breaches compared to last year's report

Fuentes: Gaceta UNAM (Dic. 11, 2025), Danielle Dithurbide (@daniellemx_), Policia de Nacional de Colombia BI: 004 y Verizon Bussiness

Opening Questions

- How are the foundational ideas of cybersecurity changing as we enter the quantum era?

Opening Questions

- How are the foundational ideas of cybersecurity changing as we enter the quantum era?
- Are our current security systems ready for a future shaped by quantum technologies?

Opening Questions

- How are the foundational ideas of cybersecurity changing as we enter the quantum era?
- Are our current security systems ready for a future shaped by quantum technologies?
- What happens to the cybersecurity concepts we learn today when quantum computers become practical?

Opening Questions

- How are the foundational ideas of cybersecurity changing as we enter the quantum era?
- Are our current security systems ready for a future shaped by quantum technologies?
- What happens to the cybersecurity concepts we learn today when quantum computers become practical?
- How do classical security principles translate into quantum cryptography in a post-quantum world?

Opening Questions

- How are the foundational ideas of cybersecurity changing as we enter the quantum era?
- Are our current security systems ready for a future shaped by quantum technologies?
- What happens to the cybersecurity concepts we learn today when quantum computers become practical?
- How do classical security principles translate into quantum cryptography in a post-quantum world?
- What role will quantum computing and machine learning play in the next generation of secure systems?

Opening Questions

- How are the foundational ideas of cybersecurity changing as we enter the quantum era?
- Are our current security systems ready for a future shaped by quantum technologies?
- What happens to the cybersecurity concepts we learn today when quantum computers become practical?
- How do classical security principles translate into quantum cryptography in a post-quantum world?
- What role will quantum computing and machine learning play in the next generation of secure systems?
- How will quantum technologies change the way we protect information in everyday life?

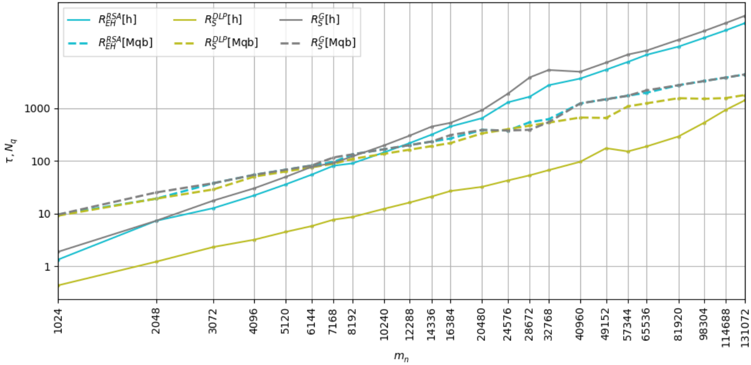
Classical concepts

Information security, Cryptology, and Cryptography are different concepts.

Definition 1 (Information security)

The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability .

Why should we be worried about QC?



“The estimation: factoring a 2048 bit integer will take approximately 7 hours, assuming only one run of the quantum part of the algorithm is needed.” arXiv:1905.09749v3

Classical concepts (cont.)

Definition 2 (Cryptology)

The science that deals with hidden, disguised, or encrypted communications. It includes communications security and communications intelligence.

Classical concepts (cont.)

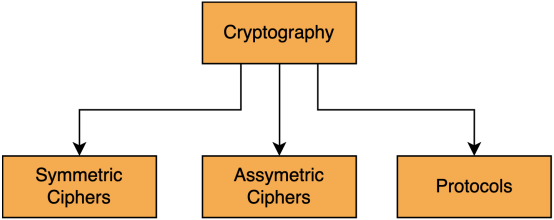
Definition 3 (Cryptography)

Literature shows different definitions, and some of these are

- The art and science of using mathematics to secure information and create a high degree of trust in the electronic realm.
- It is the science of secret writing to hide the information .

Classical concepts: Cryptography (cont.)

Cryptography is a subfield of cryptology.



Classical concepts (cont.)

Definition 4 (Shannon Entropy)

It is given by

$$S = -\sum_{i=1}^{k} p_i \log_2 p_i \tag{1}$$

The entropy of uncertainty of a random variable X with probabilities $p_i, \ldots, p_n$.

Classical concepts (cont.)

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 (bit)

The fundamental unit of classical information.

Part I. Quantum Concepts

Definition 7 (Hilbert space)

It is an abstract space where some vectors live and are represented by $|v\rangle$. The Hilbert space has the same properties as a vector space, but we also allow **complex numbers.**

Quantum Concepts (cont.)

Definition 8 (Basis)

It is a set of vectors that define a space.

1. **Orthogonal**. The dot product is defined as zero between two different vectors in the basis.
2. **Nonorthogonal**. The dot product is defined as nonzero between two different vectors in the basis.
3. **Canonical and noncanonical**. Bases such as $\{|0\rangle, |1\rangle\}$ are called canonical, and (Bell) bases such as $\left\{\frac{|0\rangle+|1\rangle}{\sqrt{2}}, \frac{|0\rangle-|1\rangle}{\sqrt{2}}\right\}$ is a noncanonical basis.

Quantum Concepts (cont.)

Definition 9 (Von Neumann Entropy)

In the quantum information context,

$$H_V = -\sum_{i=1}^{n} \lambda_i \log_2 \lambda_i \tag{2}$$

Where λ_i are the **eigenvalues** of a **density operator**.

Quantum Concepts (cont.)

Definition 10 (Eigenvalues)

It is a number $\lambda \in \mathbb{C}$ such that $AV = \lambda V$ where A is a matrix, and V is the eigenvector.

To define the density operator, we need an ensemble concept.

Definition 11 (Ensemble)

It is a collection of identically prepared physical systems. We will use $|\psi_i\rangle$ to represent an ensemble of all members.

Definition 12 (Density operator)

It is given by $\rho \equiv \sum_i p_i |\psi_i\rangle \langle\psi_i|$, and it represents an ensemble (see Definition 11) p_i is the probability to $i-$th state.

Concepts for encryption I

Definition 13 (Trapdoor function, trapdoor one-way function)

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

1. There exists a **polynomial-time algorithm** A such that $A(x) = f(x)$ for every $x \in \{0,1\}^*$.

   It means:
   A function that is easy to compute yet hard to invert without extra information is called a **trapdoor function** .

Concepts for encryption II

Definition 14 (Trapdoor function, trapdoor one-way function)

A function $f : \{0,1\}^* \to \{0,1\}^*$ is called **one-way** if the following two conditions hold,

2. For every **probabilistic polynomial-time algorithm** A', every polynomial p, and all sufficiently large n,

$$\Pr[A'(f(x), 1^n) \in f^{-1}(f(x))] < \frac{1}{p(n)}. \tag{3}$$

It means:
A function that is easily computed, and the calculation of its inverse is infeasible unless certain privileged information is known.

(some) Concepts

Definition 15 (One-Time-Pad protocol)

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

Example: One-time-Pad protocol

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 should notice

$$\begin{aligned} B = DEC(C,K) &= DEC(ENC(B,K),K) \\ &= DEC(B \oplus K, K) \\ &= B \oplus K \oplus K \\ &= B \end{aligned} \tag{4}$$

Example: Symmetric cipher

1. Encryption: To get the ciphertext, C

$$C = ENC(B,K) = B \oplus K \quad = \quad \begin{array}{cc} & b_5\, b_4\, b_3\, b_2\, b_1\, b_0 \\ \oplus & k_5\, k_4\, k_3\, k_2\, k_1\, k_0 \\ \hline & c_5\, c_4\, c_3\, c_2\, c_1\, c_0 \end{array} \tag{5}$$

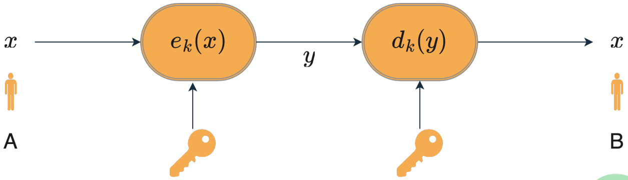


Figure: Scheme to represent the symmetric key.

Example: Symmetric cipher (cont.)

2. Decryption: To get the text, B

$$B = DEC(C, K) = C \oplus K \quad = \quad \begin{array}{r} c_5\, c_4\, c_3\, c_2\, c_1\, c_0 \\ \oplus \quad k_5\, k_4\, k_3\, k_2\, k_1\, k_0 \\ \hline b_5\, b_4\, b_3\, b_2\, b_1\, b_0 \end{array} \tag{6}$$

Example: Symmetric cipher (cont.)

1. Encryption.

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

2. Decryption

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

Q|Mexico⟩

qaldas

Part II. Quantum Concepts

Definition 16 (Quantum key exchange (QKE))

It is the idea of exploiting quantum mechanics to improve classical protocols (see Definition 19).

Part II. Quantum Concepts (cont.)

Definition 17 (BB84 protocol)

Let A and B use two points to send information, which should be two people; person A implements two different orthogonal bases (see Definition 8) to send information.

This idea formed the basis of the first quantum key exchange (QKE) protocol. An orthogonal base example is,

$$\{|\rightarrow\rangle, |\uparrow\rangle\} = \left\{[1,0]^T, [0,1]^T\right\}.$$

and

$$\{|\nwarrow\rangle, |\nearrow\rangle\} = \left\{\frac{1}{\sqrt{2}}[-1,1]^T, \frac{1}{\sqrt{2}}[1,1]^T\right\}.$$

Part II. Quantum Concepts (cont.)

Definition 18 (B92 protocol)

This protocol implements one nonorthogonal basis (see Definition 8) to send information .

An example of nonorthogonal basis,

$$\{| \rightarrow\rangle |, \nearrow\rangle\} = \left\{[1,0]^T, \frac{1}{\sqrt{2}}[1,1]^T\right\}.$$

Part II. Quantum Concepts: Applications

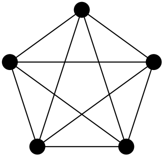
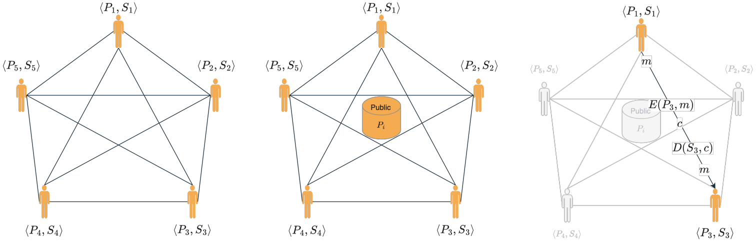


Figure: Graph for $n = 5$ and $k = 2$: This represents a network with $n = 5$ users, where $k = 2$ users are engaged in pairwise communication.

- We will swap points and
- edges

Part II. Quantum Concepts: Applications (cont.)

Graph for $n = 5$, $k = 2$ and 10 edges.


$\langle P_1, S_1\rangle$
$\langle P_5, S_5\rangle$
$\langle P_2, S_2\rangle$
$\langle P_4, S_4\rangle$
$\langle P_3, S_3\rangle$
$\langle P_1, S_1\rangle$
$\langle P_5, S_5\rangle$
$\langle P_2, S_2\rangle$
Public
P_i
$\langle P_4, S_4\rangle$
$\langle P_3, S_3\rangle$
$\langle P_1, S_1\rangle$
$\langle P_5, S_5\rangle$
$\langle P_2, S_2\rangle$
m
Public
P_i
$E(P_3, m)$
c
$D(S_3, c)$
m
$\langle P_4, S_4\rangle$
$\langle P_3, S_3\rangle$

This subsection presents the basic ideas of RSA encryption.

Cryptography, QC & AI

Definition 19 (Activation Functions)

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

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

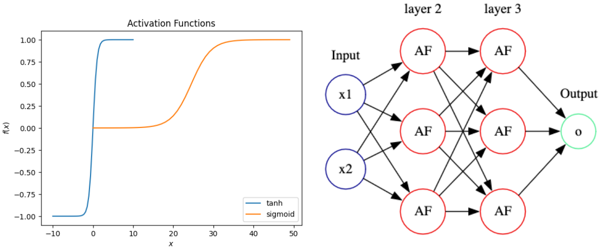


Figure: Examples of Activation functions and a fully connected network.

Neural Networks and Cryptography

Theorem 20 (Cybenko)

Let $f : \mathbb{R}^d \to \mathbb{R}$ *be a function*[a] *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* $\sigma : \mathbb{R} \to \mathbb{R}$ *is an activation function*[b]*, such that*

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

[a] continuous

[b] non-polynomial non-linear

Examples: Activation Function

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

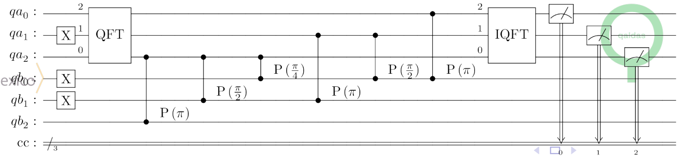
$$\sigma(x) = \mathrm{sigmoid}(x) = \frac{1}{1 + e^{-x}}$$

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

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

Figure: WebBook: QC

Figure: NB with the addition using QFT.



Conclusions and Discussion

- These slides 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 security implications.

Future directions

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

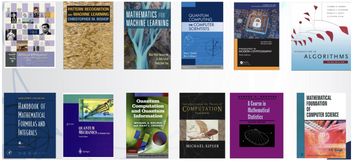
Explore and implement other options/circuits.

Figure: Repository: https://github.com/jaorduz/QCandAI

References and acknowledge

Universidad Veracruzana

Dirección
Facultad de Estadística e Informática
Región Xalapa


Pattern Recognition and Machine Learning
Christopher M. Bishop
Mathematics for Machine Learning
Quantum Computing for Computer Scientists
Introduction to Modern Cryptography
Introduction to Algorithms
Handbook of Mathematical Formulas and Integrals
Quantum Mechanics
Quantum Computation and Quantum Information
Introduction to the Theory of Computation
Michael Sipser
A Course in Mathematical Statistics
Mathematical Foundation of Computer Science

Thanks to organizers, Universidad Veracruzana for having me and their support.
JO acknowledges FESAc-UNAM, Qaldas, QWorld/QMexico for their support and chances.
JO: This paper was published as: Mathematical Foundations for Modern Cryptography in the AI. Authored by JO.