Mathematical foundations for Modern Cryptography in the Quantum Era

Javier Orduz

[1]EC, Qmexico[2]

13

December 12, 2024

1 Contents

2 Objectives

3 Concepts

4 Protocols and methods for encryption

- One-Time-Pad protocol

5 Toy model

Objectives

Objective

To show the most relevant concepts for cybersecurity and explore their counterpart in the quantum context.

(some) 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 .

(some) Concepts

Definition 2 (Cryptology)

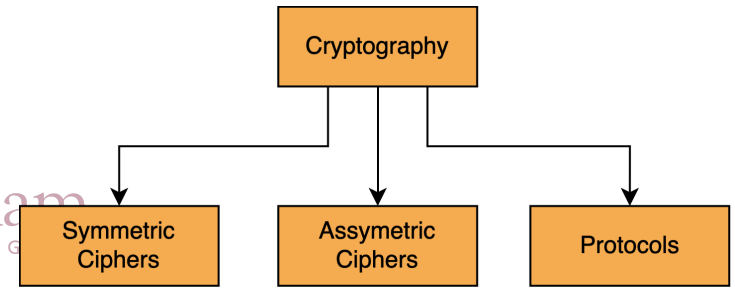
Initially, the field encompassed both **cryptography** and **cryptanalysis.** Today, cryptology in the U.S. Government is the collection and/or exploitation of foreign communications and non-communications emitters, known as SIGINT, and solutions, products, and services to ensure the **availability**, **integrity**, **authentication**, **confidentiality**, and **non-repudiation** of national security telecommunications and information systems, known as IA.

(some) Concepts

Definition 3 (Cryptography)

Literature shows different definitions, and some of these are

- The discipline that embodies the principles, means, and methods for transforming data to hide their semantic content, prevent unauthorized use or prevent undetected modification .
- It is the science of secret writing to hide the information .



(some) Concepts

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 $p_i, \ldots, p_n$.

(some) Quantum Concepts

Definition 5 (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.**

(some) Concepts

Definition 6 (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 $\left\{ \frac{|0\rangle+|1\rangle}{\sqrt{2}}, \frac{|0\rangle-|1\rangle}{\sqrt{2}} \right\}$

(some) Quantum Concepts

Definition 7 (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 .

(some) Concepts

Definition 8 (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 $x \in \{0,1\}^*$
2. For every **probabilistic polynomial-time algorithm** A', every polynomial p, and all sufficiently large n,

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

(some) Concepts (Continued)

Definition 9 (Trapdoor function, trapdoor one-way function)

We additionally have the following two definitions,

1. A function that is easy to compute yet hard to invert without extra information is called a **trapdoor function** .
2. A function that is easily computed, and the calculation of its inverse is infeasible unless certain privileged information is known.

(some) Concepts

Definition 10 (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** .

(some) Concepts

Definition 11 (One-Time-Pad protocol)

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

(some) Quantum Concepts (Continued)

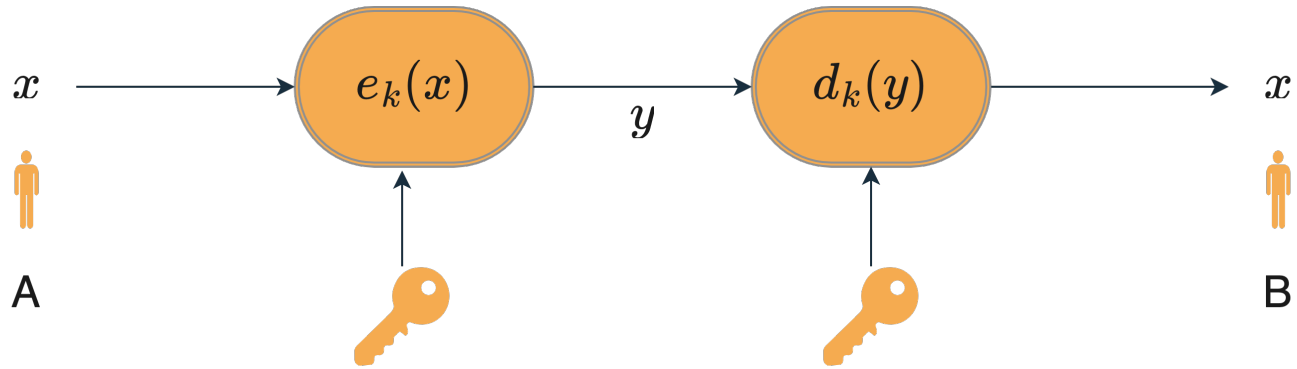
We use B the text in binary is H= $1001000_2 = 72_{10}$ and ciphertext in binary system is Z= $1011010_2 = 90_{10}$. The subscripts refer to binary and decimal systems.
We should notice

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

Example

1. Encryption: To get the ciphertext, C

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



Example (continued)

2. Decryption: To get the text, B

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

Example (continued)

1. Encryption.

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

2. Decryption

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

(some) Quantum Concepts

Definition 12 (Quantum key exchange (QKE))

It is the idea of exploiting quantum mechanics to improve classical protocols (see Definition 10).

Definition 13 (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 6) to send information.

Definition 14 (B92 protocol)

This protocol implements one nonorthogonal basis (see Definition 6) to send information .

Applications

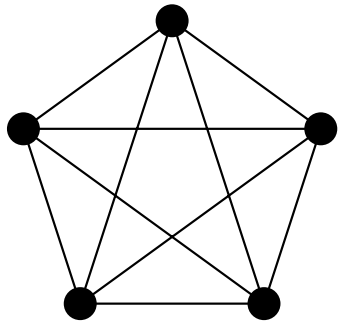
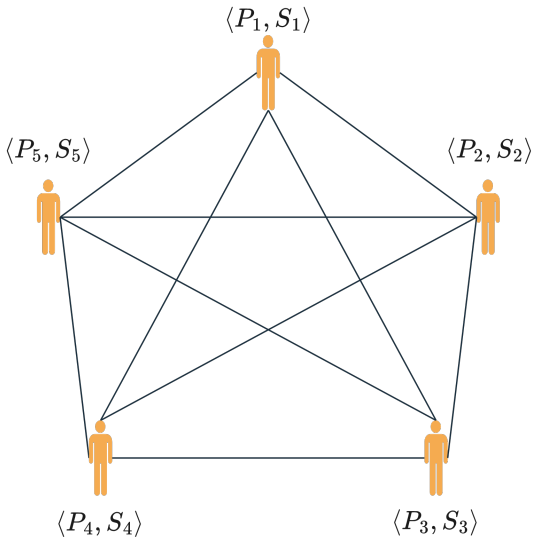
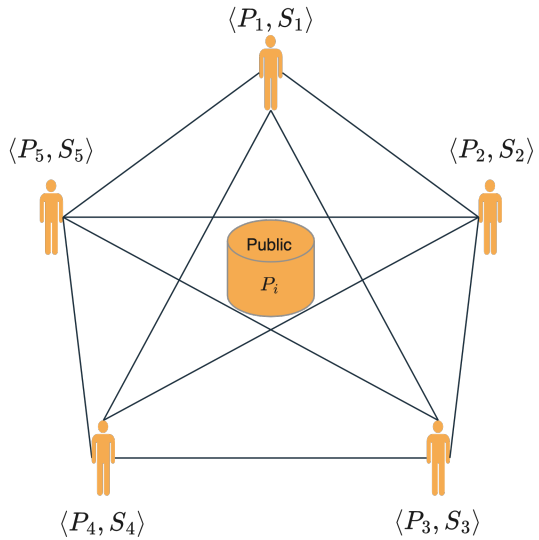


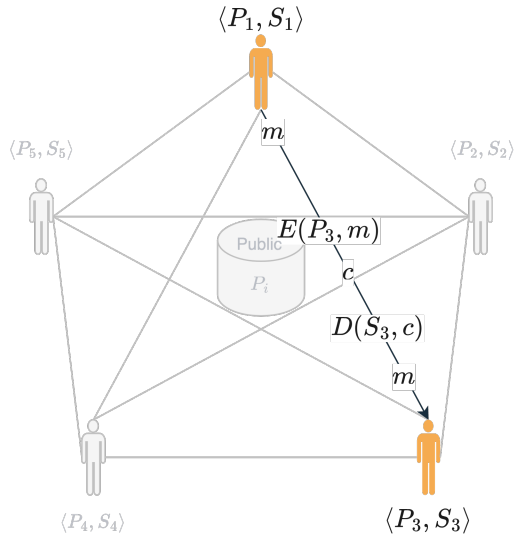
Figure: Graph for $n = 5$ and $k = 2$: This represents a network with $n = 5$ users, where $k = 2$ users are engaged in pairwise communication.

- We will swap points and
- edges

Applications (continued)







Mexico

Earlham COLLEGE

Conclusions and Discussion

- This paper examined key concepts in cybersecurity and their counterparts in the quantum domain.
- It also provided foundational insights into prominent protocols in classical and quantum cryptography.

Future directions

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.

Thank you!