Essential Mathematical Tools for Modern Cryptography

Levi Goldberg and Javier Orduz

Department of Mathematics, Earlham College

Earlham COLLEGE

Abstract and Objectives

This poster presents a comprehensive overview of fundamental technical concepts from computer science and mathematics for the next generation of scientists in the cryptography field. **Objectives**

- Collect and present relevant theorems, lemmas, and definitions from both mathematics and physics, highlighting their quantum counterparts where applicable.

General Definitions

Definition 0.1 (Information security)

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

Definition 0.2 (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.

Definition 0.3 (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 .

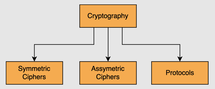
Definition 0.4 (Shannon Entropy)

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 $p_i, \ldots, p_n$.

Introduction to Computing and Quantum Computation



Quantum computers can overcome classical computers and bring potential vulnerabilities to our systems. This poster aims to outline fundamental concepts in cryptography, which are essential for aspiring computer scientists in the post-quantum era. We present a curated list of fourteen key definitions from both classical and quantum cryptography.

Classical Definitions

Definition 0.5 (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.**

Definition 0.6 (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 $\left\{\frac{|0\rangle+|1\rangle}{\sqrt{2}}, \frac{|0\rangle-|1\rangle}{\sqrt{2}}\right\}$

Definition 0.7 (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 .

Modern Definitions: Quantum context

Definition 0.8 (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,

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

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.

Definition 0.9 (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 0.10 (One-Time-Pad protocol)

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

Definition 0.11 (Quantum key exchange (QKE))

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

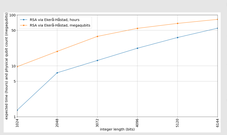
Definition 0.12 (BB84 protocol)

Let A and B use two points to send information which should be two people; person-A implements two different orthogonal bases to send information.

Definition 0.13 (B92 protocol)

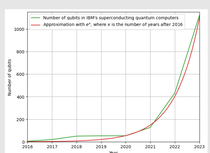
This protocol implements one nonorthogonal basis to send information .

Quantum vs. Classical computers



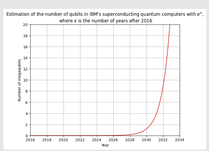
The time and qubit requirements for a quantum computer to factor integers of various lengths. 2048-bit integers, which many modern encryptions use, could be broken by a quantum computer with 20 Mqubits (20 million qubits) in about 7 hours.

Prediction: Superconducting quantum computers



The number of qubits in International Business Machine (IBM)'s most powerful quantum computers each year from 2016 to 2023 (green). This graph closely matches that of the function e^x, where x is the number of years after 2016 (red). This means that the function e^{x-2016} can be used to predict how many qubits IBM's most powerful machines will have in any year x. Made with data from (4).

Prediction to reach 20 Mqb



The predictive function for the number of megaqubits in IBM's most powerful quantum computers from the above graph extended to the year 2034. If IBM continues to advance its technology at the same rate, then it will reach 20 megaqubits around the year 2033. This means that any data encrypted with a 2048-bit or less integer would be vulnerable.

Acknowledgements & References: Thanks to Earlham College for partially funding this project through the Stephen and Sylvia Tregidga Burges Endowed Fund for Student-Faculty Collaborative Research. JO acknowledges support from APS through award 9615914607. References will be included in the final paper: Mathematical foundations for Modern Cryptography in the Quantum Era. Authored by JO.

Q|Mexico