Optimization of the McEliece Cryptosystem

David Lázaro Rodríguez Lima

Polytechnic School of Engineering of Vilanova i la Geltrú
Department of Electronic Engineering

18 de mayo de 2023

UNIVERSITAT POLITÈCNICA DE CATALUNYA
BARCELONATECH
Escola Politècnica Superior d'Enginyeria
de Vilanova i la Geltrú

Content

UNIVERSITAT POLITÈCNICA DE CATALUNYA
BARCELONATECH
Escola Politècnica Superior d'Enginyeria
de Vilanova i la Geltrú

Content

UNIVERSITAT POLITÈCNICA DE CATALUNYA
BARCELONATECH
Escola Politècnica Superior d'Enginyeria
de Vilanova i la Geltrú

- Is the basis of any computer security mechanism.
- Cryptographers research, develop and use mathematical techniques that provide an improvement in the implementation and execution of the cryptosystem providing greater security.
- The main objective is to achieve a cryptographic key, complex enough, so that it is very unlikely that a third party can crack the encrypted text with brute force, runtime attacks or other types of attacks.
- There are two types of encryption: **symmetric encryption** (same public key and private key) and **asymmetric encryption** (different public key and private key).

- Postquantum cryptography is a branch of cryptography that works on the design of encryption algorithms resistant to quantum algorithms.
- Shor's algorithm and Grover's algorithm are examples of quantum algorithms that would break currently used cryptographic algorithms (RSA, AES) when quantum computers are a reality.
- Mceliece's cryptosystem is an encryption algorithm used due to the great security it provides.

The McEliece cryptosystem was proposed in 1978 by Robert McEliece. This cryptosystem is asymmetric encryption based on the Algebraic Coding Theory. It was the first scheme to use the randomization in the encryption process. This has three phases:

1. Key generation (Theoretically and computationally most expensive phase)
2. Encryption process.
3. decryption process.

Post-quantum cryptography standardization process of the National Institute of Standards and Technology (NIST).

Introduction and background

NIST

- NIST created a working group on post-quantum cryptography in 2012, motivated by advances in quantum computing and the threats that these advances represent for TICs.
- In 2016, NIST, following the instructions of the United States National Security Agency (NSA) (2015) launched an open competition for the standardization of post-quantum cryptography.
- In this contest, 69 works passed the first round. Currently a cryptosystem based on the McEliece cryptosystem is among the finalists. This work is titled **Classic McEliece**.

- Classic McEliece is a cryptosystem where each level of the construction is designed so that future cryptographic auditors can rely on the long-term security of post-quantum public-key cryptographic encryption.
- It is designed to send small messages due to the key size of McEliece's original cryptosystem.
- It has a large number of collaborators from universities and technology centers from different parts of the world.
- the cryptosystem has a website: *https://classic.mceliece.org*, where the latest and innovative papers are freely available. They also have 4 different free software and hardware implementations.

Why the McEliece Cryptosystem?

Advantages

- It solves the main disadvantage of symmetric encryption: the problem of sharing the unique key.
- It is the cryptosystem that has been tested the most. Postquantum security is guaranteed by the many failed attacks.

Disadvantages

The disadvantages are mainly due to the large size of the keys.

- The high execution time.
- Large memory space consuming.

Problems

- The disadvantages cause that the cryptosystem could not be executed for large parameters due to the time it takes and the memory capacity it requires.
- There are attacks according to the execution time, which can break algorithms that their execution is not in constant time.

Objectives

- Develop and implement, in constant time, more efficient algorithms for the reduction of execution time and the size of the keys.
- Implement an efficient biometric cryptosystem based on the McEliece cryptosystem.

Content

UNIVERSITAT POLITÈCNICA DE CATALUNYA
BARCELONATECH
Escola Politècnica Superior d'Enginyeria
de Vilanova i la Geltrú

- The methodology consists of the study of code theory and the different algebras, especially Galois theory, to create more efficient algorithms. The efficiency of these new algorithms is verified with the theoretical comparison of the operational order, the comparison of the execution time in its software implementation and the use of probability theory to verify the security levels.
- In the three phases of the cryptosystem, low-level and high-level algorithms are used:
  - Low-level algorithms are operations on finite fields and on extensions of finite fields: addition, multiplication, inverse, division, power, root.
  - High-level algorithms include: obtaining irreducible polynomials, obtaining separable polynomials, evaluation of polynomials, error-correcting algorithms.

An important step in the key generation phase is obtaining an irreducible or separable polynomial. Authors use the two types of polynomials. The current algorithm used to obtain irreducible polynomials is more efficient than the algorithm to obtain a separable polynomial.

Definition

Irreducible polynomials are separable over finite fields.

Definition

Minimal polynomials are irreducible.

The following theorem is an important result and needs several definitions on Galois theory to obtain its proof.

Theorem

The multiplication of minimal polynomials is a polynomial separable.

This theorem allows me to apply the principle "divide and conquer".
The computational complexity of the algorithm to find irreducible polynomials is the same computational complexity of Gaussian elimination: $O(t^3)$, t is the degree of the polynomial and represents a matrix of $t \times t$ in the algorithm .
Applying the theorem I can find polynomials of lower degree, such that their multiplication is a separable polynomial of the needed degree. This is how I reduce computational complexity.

Theorem

Let $g(x)$ be a polynomial such that $g(x) = \prod_{i=1}^{n} g_i(x)$, the degree of $g(x)$ is t and the degree for each $g_i(x)$ is equal to t/n. The computational complexity of obtaining $g(x)$ using the algorithm to obtain the irreducible polynomial is $O(t^3)$. Then the number of operations that the algorithm performs on the n polynomials $g_i(x)$ is $O(t^3)/n^2$.

Proof:

The computational complexity of Gaussian elimination is $O(t^3)$ for matrices of $t \times t$ so the computational complexity for matrices of dimension $(t/n \times t/n)$ is $O((t/n)^3)$. Adding the orders of operations, we get:

Methodology and results

Example of result obtained

$$\underbrace{\left(\frac{t}{n}\right)^3 + \left(\frac{t}{n}\right)^3 + \ldots + \left(\frac{t}{n}\right)^3}_{n-veces}$$

$$= \underbrace{\frac{t^3}{n^3} + \frac{t^3}{n^3} + \ldots + \frac{t^3}{n^3}}_{n-veces}$$

$$= \frac{nt^3}{n^3}$$

$$= \frac{t^3}{n^2}$$

UNIVERSITAT POLITÈCNICA DE CATALUNYA
BARCELONATECH
Escola Politècnica Superior d'Enginyeria
de Vilanova i la Geltrú

Methodology and results

Example of result obtained

- These results in which computational complexity is reduced lead to an analysis to see if computational security is affected. For this, brute force attacks are simulated and the probability of success is calculated. Each parameter in the algorithm must have 256-bit security.
- These algorithms also need vectorized implementations in C to take full advantage of the properties of the computer.