UNIVERSIDAD POLITÉCNICA DE MADRID

ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA Y DISEÑO INDUSTRIAL

Grado en Ingeniería Electrónica Industrial y Automática

TRABAJO FIN DE GRADO

Estudio comparativo de diferentes algoritmos de encriptación para comunicaciones industriales

Bogurad Barañski Barañska

Tutor: Roberto Gonzalez Herranz
Departamento: ingeniería eléctrica, electrónica, automática y física aplicada.

Madrid, Mes, 2025

UNIVERSIDAD POLITÉCNICA DE MADRID

ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA Y DISEÑO INDUSTRIAL

Grado en Ingeniería Electrónica Industrial y Automática

TRABAJO FIN DE GRADO

Título del trabajo

Firma Autor

Firma Tutor

Título: Estudio comparativo de diferentes algoritmos de encriptación para comunicaciones industriales
Autor: Bogurad Barañski Barañska
Tutor: Roberto Gonzalez Herranz

EL TRIBUNAL

Presidente:

Vocal:

Secretario:

Realizado el acto de defensa y lectura del Trabajo Fin de Grado el día ..... de ..... de ... en ....., en la Escuela Técnica Superior de Ingeniería y Diseño Industrial de la Universidad Politécnica de Madrid, acuerda otorgarle la CALIFICACIÓN de:

VOCAL

SECRETARIO PRESIDENTE

Agradecimientos

Agradezco a .....

Resumen

Este proyecto se resume en.....

Palabras clave: palabraclave1, palabraclave2, palabraclave3.

Abstract

In this project...

Keywords: keyword1, keyword2, keyword3.

Índice general

Índice de figuras

Índice de tablas

Capítulo 1

Introducción

1.1. Motivación del proyecto

Cuando en una instalación industrial se actúa o se mide un proceso, el autómata que envía las señales puede estar situado a gran distancia de dicho proceso. Por esta razón, las comunicaciones industriales precisan el uso de buses de longitudes considerables o realizar comunicaciones a distancia.

Aunque las comunicaciones a distancia pudieran parecer una solución más económica de implementar, tienen el problema de ser vulnerables a ataques de intermediario (alguien ajeno al proceso intercepta los mensajes enviados), lo cual pone en peligro la confidencialidad de la información. Por esta misma razón, en este trabajo se estudiarán distintos algoritmos propuestos para la encriptación de los mensajes.

1.2. Objetivos

Para realizar el proyecto, se proponen los siguientes objetivos:

- Implementar los siguientes algoritmos en C/C++
  - RSA
  - Curvas elípticas
  - AES 256
  - Celosías
  - Algoritmo de Shore
  - Algoritmos post-cuánticos
- Estudiar la eficacia de cifrado
  - Estudiar velocidad de ejecución del algoritmo
  - Estudiar recursos requeridos por el microprocesador
  - Estudiar la robustez del cifrado
  - Estudiar la posibilidad de ataques de canal lateral
- Posibilidad de ejecución en sistemas basados en FPGAs

- Qué y cómo medir en las ECC Intercambio de claves pública privado mediante RSA/ leif-haunman
  - Capacidad de memoria
  - Tiempo de CPU
  - Estudio de entropía

1.3. Herramientas utilizadas

1.3.1. LaTex [1]

Se ha preferido el uso de LaTeX debido a la facilidad que ofrece para el maquetado de textos, superando a otras herramientas de elaboración de documentos. Además, LaTeX permite crear figuras vectorizadas, representar correctamente ecuaciones y ubicar adecuadamente figuras, tablas y bibliografía.

1.3.2. TikzMaker [2]

Esta herramienta permite crear figuras vectorizadas de LaTeX mediante el paquete de circuitikz. Su principal ventaja radica en la interfaz gráfica que proporciona y en la facilidad para elaborar figuras.

1.3.3. C y C++

1.3.4. Microprocesador CY8CPROTO-063-BLE

1.4. Estructura del documento

A continuación y para facilitar la lectura del documento, se detalla el contenido de cada capítulo:

- En el capítulo 1 se realiza una introducción.
- En el capítulo 2 se hace un repaso de desarrollos anteriores .
- En el capítulo 3 se desarrollan los fundamentos matemáticos del proyecto.
- En el capítulo 4 se describe la implementación de los algoritmos.
- En el capítulo 5 se exponen los resultados obtenidos en el capítulo anterior.
- En el capítulo 6 se comparan los resultados de los distintos algoritmos.

Capítulo 2

Estado del arte

Capítulo 3

Fundamentos generales

En este capítulo se desarrollan las bases matemáticas de los distintos algoritmos a implementar.

3.1. Introducción

3.2. Algoritmos de Hashing y Funciones de Salida Extendida[3]

3.3. Métodos clásicos de cifrado asimétrico

3.3.1. RSA

3.3.2. ECC

3.3.3. Algoritmo de Shore

3.4. Funcionamiento básico de los algoritmos postcuánticos

En esta sección se describe el funcionamiento de los algoritmos postcuánticos analizados en este trabajo. Dado que no se desarrollaron implementaciones propias, sino que se utilizó el código proporcionado por el NIST en la tercera [4] y cuarta [5] ronda del proceso de estandarización, resulta apropiado presentar su funcionamiento aquí en lugar de en la sección de desarrollo.

3.4.1. CRYSTALS-Kyber

Para [6]

3.4.2. SABER

Para [7]

3.4.3. Hamming Quasi-Cyclic (HQC)

Para [8]

3.4.4. Bit Flipping Key Encapsulation (Bike)

Para [9]

3.5. Fundamentos de seguridad de los algoritmos

3.5.1. CRYSTALS-Kyber

Para [6]

3.5.2. SABER

Para [7]

3.5.3. Hamming Quasi-Cyclic (HQC)

Para [8]

3.5.4. Bit Flipping Key Encapsulation (Bike)

Para [9]

Capítulo 4

Desarrollo

4.1. Implementación comunicación serie

4.1.1. Parámetros generales y formato mensajes

4.1.2. Implementación en el ordenador

4.1.3. Implementación en el microprocesador

4.2. Implementación algoritmos de cifrado asimétrico

4.2.1. Kyber

4.2.2. Saber

4.2.3. Bike

4.2.4. HQC

4.3. Implementación del intercambio de claves. Creación del secreto compartido

Capítulo 5

Resultados y discusión

En este capítulo se muestran los resultados obtenidos de aplicar las rutinas desarrolladas con anterioridad.

5.1. Resultados

5.2. Discusión

Capítulo 6

Conclusiones

Se presentan a continuación las conclusiones del proyecto y desarrollos futuros para mejorar la implementación.

6.1. Conclusión

Una vez finalizado el proyecto...

6.2. Desarrollos futuros

Un posible desarrollo...

Apéndice A

Definiciones básicas

Bibliografía

[1] Leslie Lamport et al. The latex project, 2024.

[2] Tikzmaker. https://tikzmaker.com/editor, 2024.

[3] National Institute of Standards, Technology (NIST), and Morris J. Dworkin. Sha-3 standard: Permutation-based hash and extendable-output functions, 2015-08-04 00:08:00 2015.

[4] National Institute of Standards and Technology. Post-quantum cryptography - round 3 submissions. https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization/round-3-submissions, 2020. Consultado: 2025-05-05.

[5] National Institute of Standards and Technology. Post-quantum cryptography - round 4 submissions. https://csrc.nist.gov/Projects/post-quantum-cryptography/round-4-submissions, 2022. Consultado: 2025-05-05.

[6] Roberto Avanzi, Joppe Bos, Léo Ducas, Eike Kiltz, Tancrède Lepoint, Vadim Lyubashevsky, John M. Schanck, Peter Schwabe, Gregor Seiler, and Damien Stehlé. CRYSTALS-Kyber: Algorithm Specifications and Supporting Documentation (version 3.01). Technical report, CRYSTALS Project, January 2021. NIST PQC Round 3 submission.

[7] Andrea Basso, José María Bermudo Mera, Jan-Pieter D'Anvers, Angshuman Karmakar, Sujoy Sinha Roy, Michiel Van Beirendonck, and Frederik Vercauteren. SABER: Mod-LWR based KEM (Round 3 Submission). Technical report, Katholieke Universiteit Leuven and University of Birmingham, 2020. NIST PQC Round 3 submission.

[8] Carlos Aguilar Melchor, Nicolas Aragon, Slim Bettaieb, Loïc Bidoux, Olivier Blazy, Jurjen Bos, Jean-Christophe Deneuville, Arnaud Dion, Philippe Gaborit, Jérôme Lacan, Edoardo Persichetti, Jean-Marc Robert, Pascal Véron, and Gilles Zémor. HQC: Hamming Quasi-Cyclic (Fourth Round Submission). Technical report, HQC Team, October 2022. NIST PQC Round 4 submission.

[9] Nicolas Aragon, Paulo S. L. M. Barreto, Slim Bettaieb, Loïc Bidoux, Olivier Blazy, Jean-Christophe Deneuville, Philippe Gaborit, Santosh Ghosh, Shay Gueron, Tim Güneysu, Carlos Aguilar Melchor, Rafael Misoczki, Edoardo Persichetti, Jan Richter-Brockmann, Nicolas Sendrier, Jean-Pierre Tillich, Valentin Vasseur, and Gilles Zémor. BIKE: Bit Flipping Key Encapsulation (Round 4

Submission). Technical report, BIKE Team, October 2022. NIST PQC Round 4 submission.