Comparative Analysis of Lattice-based Post-Quantum Cryptosystems

M.A. González de la Torre
L. Hernández Encinas
J.I. Sánchez García

RECSI
Santander, 20 de octubre, 2022

Instituto de Tecnologías Físicas y de la Información Technologies (ITEFI)
Consejo Superior de Investigaciones Científicas (CSIC)
C/ Serrano 144, Madrid, España

{ma.gonzalez, luis.h.encinas, ji.sanchez}@csic.es

Índice

Introducción

El Instituto Nacional de Estándares y Tecnología (NIST) norteamericano está finalizando el proceso de establecer nuevos estándares criptográficos poscuánticos en dos categorías: Mecanismos de Encapsulación de Claves (*Key Encapsulation Mechanism* o KEM) y Firmas Digitales.

Durante las diferentes fases del proceso de normalización, las propuestas presentadas han sido profundamente estudiadas, fundamentalmente en lo relativo a su seguridad y a su rendimiento.

En esta comunicación centramos nuestro trabajo en cómo los principales algoritmos basados en retículos llevan a cabo sus implementaciones. Además, comparamos cada algoritmo con los demás mediante diferentes pruebas en el mismo dispositivo, para obtener resultados lo más equiparables posible.

PQC convocatoria del NIST

Los algoritmos poscuánticos presentados al NIST en 2016 pueden ser clasificados en cinco categorías distintas, dependiendo del problema matemático en el que estén basados:

- Códigos correctores de errores.
- Funciones resumen (*hash functions*).
- Sistemas de ecuaciones cuadráticas en varias variables.
- Retículos (*lattices*).
- Isogenias entre curvas elípticas.

3ª fase: propuestas basadas en retículos

Los algoritmos basados en retículos parece que son las opciones más prometedoras.

En la tercera fase del proceso de estandarización, en la categoría de clave pública, tres de los cuatro algoritmos seleccionados están basados en retículos:

- SABER (M-LWE Rounding).
- Kyber (M-LWE).
- NTRU (SVP-NTRU).

De ellos, Kyber se ha establecido como estándar (julio de 2022).

FrodoKEM

Además de los tres algoritmos mencionados, hemos incluido FrodoKEM en nuestro estudio, que se consideró como alternativa en la tercera ronda de la convocatoria del NIST.

La seguridad de FrodoKEM es, al menos, equivalente a la de los otros algoritmos.

Según el informe de la segunda evaluación de los candidatos del NIST, los algoritmos finalistas presentaban cualidades como tiempos de ejecución más cortos o longitudes de clave más cortas, lo que los hace más atractivos cómo finalistas.

FrodoKEM se diferencia de otros algoritmos, como Kyber o SABER, en determinados aspectos matemáticos, mientras que estructuralmente son muy similares. Estos tres algoritmos basan su seguridad en el problema llamado *Learning With Errors* (LWE).

Learning With Errors (LWE)

El problema *Learning With Errors* (LWE) utilizado en FrodoKEM se enuncia de la siguiente manera:

Se considera el retículo $\mathbb{Z}_q^n$, una distribución de error, χ, y un secreto, $\mathbf{s}$. Entonces se definen $(\mathbf{a}_i, b_i)$ de la siguiente manera: $\mathbf{a}_i \leftarrow_R \mathbb{Z}_q^n$ y $b_i = \langle \mathbf{a}_i, \mathbf{s} \rangle + e_i$, donde $e_i \leftarrow_\chi \mathbb{Z}_q$.

La versión decisional del problema se plantea como sigue: dado $\mathbf{s}$, distinguir si es el secreto usado para obtener $\mathbf{b}$ en la operación $\mathbf{b} = \mathbf{A} \cdot \mathbf{s} + \mathbf{e}$ o si $\mathbf{s}$ ha sido escogido de forma aleatoria.

La versión de búsqueda del problema consiste en encontrar $\mathbf{s}$, a partir de $\mathbf{A}$ y $\mathbf{b}$, siendo:

$$\begin{aligned} \mathbf{a}_1 \in \mathbb{Z}_q^n, &\quad b_1 = \langle \mathbf{s}, \mathbf{a}_1 \rangle + e_1, \\ \mathbf{a}_2 \in \mathbb{Z}_q^n, &\quad b_2 = \langle \mathbf{s}, \mathbf{a}_2 \rangle + e_2, \\ &\vdots \\ \mathbf{a}_r \in \mathbb{Z}_q^n, &\quad b_r = \langle \mathbf{s}, \mathbf{a}_r \rangle + e_r. \end{aligned}$$

Cifrado con LWE

El problema LWE se utiliza para cifrar siguiendo el siguiente esquema:

Se definen $sk := \mathbf{s}$ y $pk := (\mathbf{A}, \mathbf{b} = \mathbf{A} \cdot \mathbf{s} + \mathbf{e})$.

Para cifrar el mensaje m, mediante una distribución de error, se generan cadenas e', s' y e''.

Se definen entonces

$$\mathbf{b}' = \mathbf{s}' \cdot \mathbf{A} + \mathbf{e}',$$
$$\mathbf{v} = \mathbf{s}' \cdot \mathbf{b} + \mathbf{e}'' + m.$$

Para descifrar m se lleva a cabo la siguiente operación:

$$\mathbf{v} - \mathbf{b}' \cdot \mathbf{s} = m + \hat{\mathbf{e}}.$$

Otros problemas sobre retículos

Kyber y SABER utilizan el retículo polinómico $\mathbb{Z}_p[x]/(x^n+1)$, para un primo p y $n \in \mathbb{Z}$, aplicando la variante del problema LWE llamada Modulo-LWE (M-LWE).

El uso de retículos polinómicos permite hacer uso de algoritmos de multiplicación de polinomios (*Number-Theoretic Transform* o NTT).

En el caso de NTRU, las operaciones y el problema subyacente son diferentes, pero reducen en seguridad al problema de retículos SVP.

FrodoKEM, por su parte, tiene un diseño conservador, que prioriza la seguridad por encima de la funcionalidad del criptosistema, trabajando en el retículo $\mathbb{Z}_q^n$.

Objetvo de seguridad del NIST

El NIST establece como objetivo de seguridad semántica la noción de Indistinguibilidad frente a ataques contra el texto cifrado (IND-CCA).

Todos los algoritmos estudiados usan una versión u otra de la Transformation de Fujisaki-Okamoto (FO) para alcanzar esta definición de seguridad.

En la seguridad se consideran tanto los modelos clásicos como cuánticos.

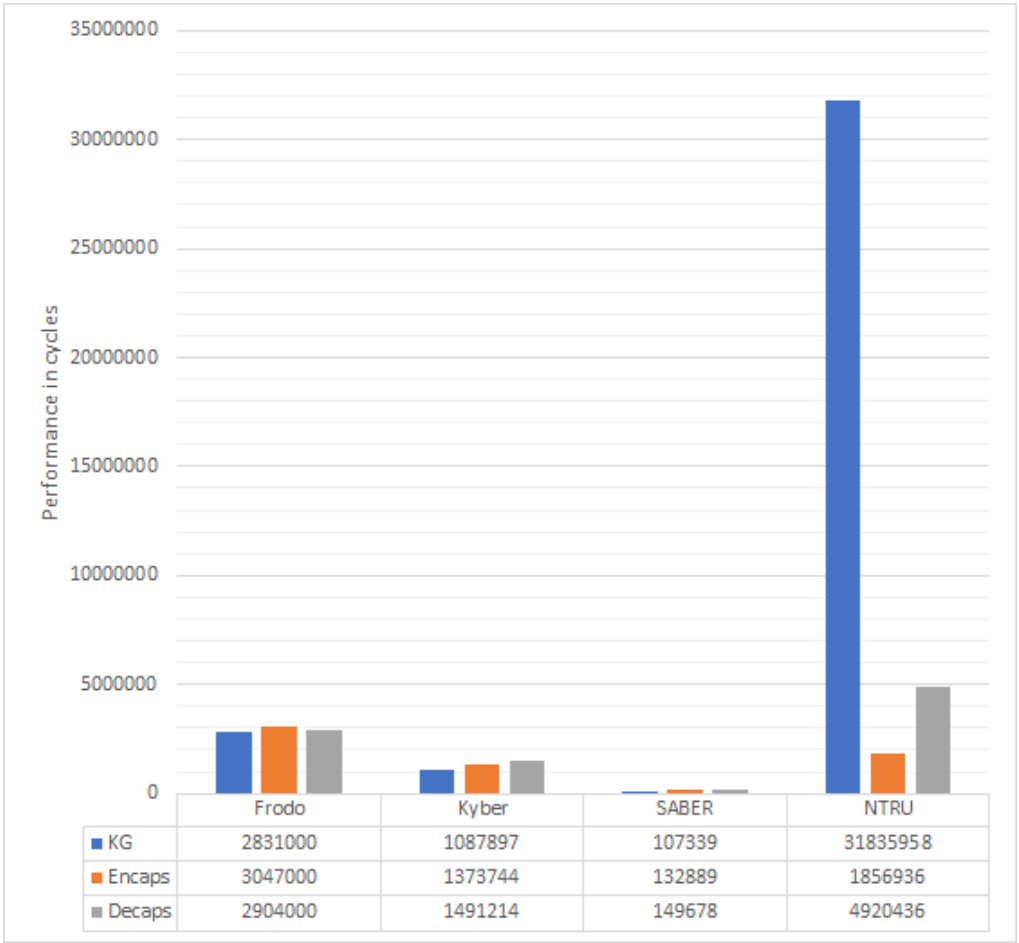
Por otro lado, dentro de la seguridad, existen ataques específicos contra alguno de los algoritmos mencionados o sus implementaciones, cuyo estudio queda fuera del objetivo de esta comunicación.

Análisis de rendimiento

Una vez estudiada la seguridad de los algoritmos y dado que todos ellos tienen la misma definición de seguridad semántica, el siguiente aspecto a analizar es su funcionalidad.

Este es el punto principal en el que se centra nuestro estudio. Para ello, en vez de usar los datos facilitados en las documentaciones oficiales de los algoritmos, hemos usado las versiones del código de referencia para estudiar su tiempo de ejecución.

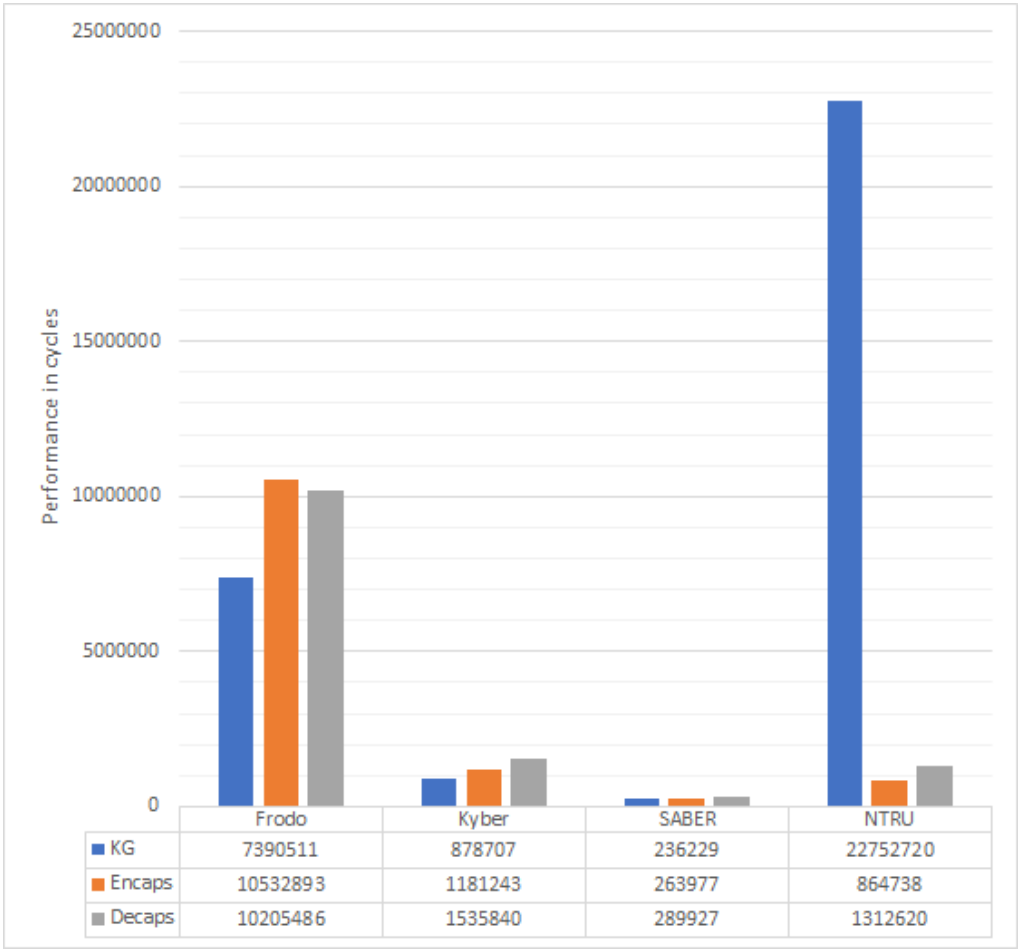
Rendimiento (ciclos)



	Frodo	Kyber	SABER	NTRU
KG	2831000	1087897	107339	31835958
Encaps	3047000	1373744	132889	1856936
Decaps	2904000	1491214	149678	4920436

Figura: Resultados de rendimiento (ciclos) aportados en las documentación de los candidatos

Rendimiento (ciclos)



	Frodo	Kyber	SABER	NTRU
KG	7390511	878707	236229	22752720
Encaps	10532893	1181243	263977	864738
Decaps	10205486	1535840	289927	1312620

Figura: Resultados de rendimiento (ciclos) obtenidos

Longitudes de claves y textos cifrados

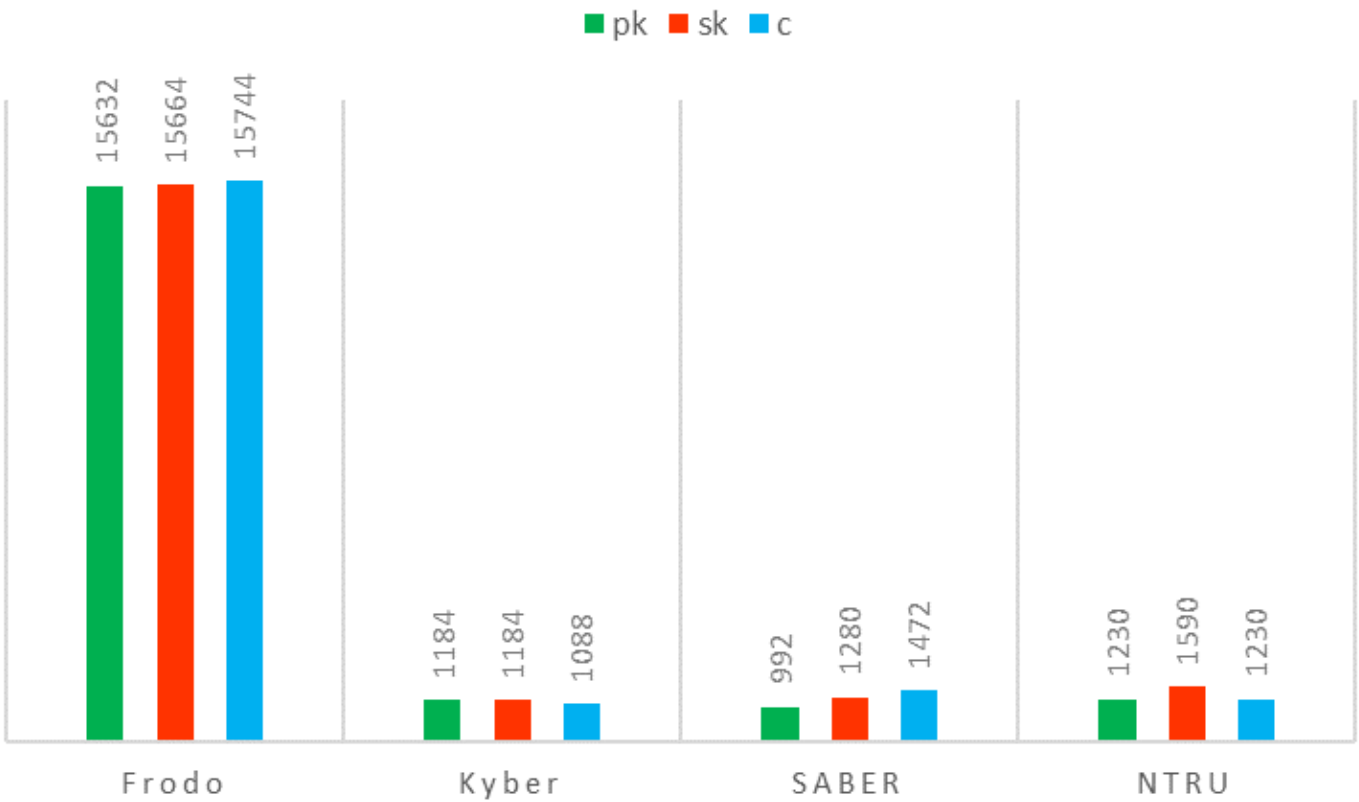


Figura: Tamaños de pares de claves y textos cifrados

Conclusiones

- Ejecutar los test en un mismo dispositivo nos da una comparativa más realista de los algoritmos y sus diferencias matemáticas.
- Podemos ver que Kyber y SABER son los algoritmos con mejores tiempos de ejecución. Lo que respalda la decisión del NIST de establecer Kyber como estándar.
- El uso de multiplicación rápida de polinomios en algoritmos como Kyber o SABER es más eficiente, debido al uso de una estructura algebraica subyacente, que en el caso de FrodoKEM, que emplea el problema clásico LWE.
- En el caso de NTRU, debido a que su estructura no se asemeja a los otros algoritmos, no es viable una comparativa directa, pero queda claro en los datos estudiados que la generación de clave supone un gran problema para las versiones software.

Trabajo futuro

- La posibilidad de ataques contra la estructura algebraica de los algoritmos basados en M-LWE puede suponer que, en un futuro, la relevancia de FrodoKEM resurja.
- El uso de primitivas establecidas por el NIST en las implementaciones presentadas al proceso de estandarización conlleva ciertas ganrantías de seguridad, pero los resultados a nivel de rendimiento se ven resntidos. Este tema ya ha sido estudiado para algunos algoritmos y se plantea como una posible línea de exploración.

Agradecimientos

Proyecto P²QProMeTe: Protocolos, Mecanismos y Tecnologías Pre y Postcuánticas para la Ciberseguridad y la Privacidad, Ref. PID2020-112586RBI00, financiado por MCIN/AEI/10.13039/501100011033

Proyecto ORACLE: Organically Resilient and Secure Wireless Networks for Next-Generation IoT Technologies to serve Future Connected Societies, Ref. PCI2020-120691-2, financiado por MCIN/AEI/10.13039/501100011033 y por la Unión Europea NextGenerationEU/PRTR

Proyecto QURSA: QUantum-based Resistant Architectures and Techniques. Integration QKD+PQC, Ref. TED2021-130369BC33, financiado por MCIN/AEI/10.13039/501100011033 y por la Unión Europea NextGenerationEU/PRTR

Proyecto CYNAMON: Cybersecurity, Network Analysis and Monitoring for the Next Generation Internet, Ref. P2018/TCS-4566-CM, financiado por la Comunidad de Madrid (Spain) and cofinanciado por European Regional Development Fund (ERDF) and European Social Fund (ESF)

Proyecto SPIRS: Secure Platform for ICT Systems Rooted at the Silicon Manufacturing Process, Ref. H2020-SU-ICT-2018-2020, financiado por la Unión Europea, Horizonte 2020

Muchas gracias por su atención

¿Preguntas?