CN-PYTEC
centro criptológico nacional

CCN-TEC 009

Recomendaciones para una transición postcuántica segura

CCN
centro criptológico nacional

Diciembre 2022

Edita:

CCN-PYTEC

Fecha de Edición: diciembre de 2022

ÍNDICE

1. INTRODUCCIÓN

1. A lo largo de los últimos años, estamos asistiendo a un importante desarrollo de la computación cuántica, siendo uno de los temas que mayor atención está despertando en la comunidad científica. Esta atención está relacionada con las enormes ventajas que supondrá la aparición de un ordenador cuántico con gran capacidad de cálculo para abordar problemas que hoy en día son de difícil solución, como los relacionados con la logística, la aeronáutica, la biotecnología, la farmacología, etc.

2. Hasta la fecha nadie se ha comprometido a dar una fecha exacta de cuándo una computación cuántica relevante será realidad. Desde hace unos años se viene diciendo que dentro de 20-25 años esta computación estará disponible, pero los años pasan y este plazo futuro no se modifica. Los más optimistas apuntan a que a finales de la década de los 30 podríamos tener una computación cuántica con elevado poder de cálculo, pero no hay evidencias claras de ello.

3. Otro de los aspectos en los que los avances en la computación cuántica tendrán una enorme repercusión en nuestras vidas son los relacionados con la seguridad, protección y custodia de la información. En este caso se trata de que tal poder de cálculo podrá resolver la mayor parte de los problemas matemáticos en los que se basa la seguridad de la criptografía actual, dejándola indefensa, esto es, permitiendo que el acceso a la información confidencial pase a ser una realidad. En otras palabras, la criptografía tal y como la conocemos hoy en día, dejará de cumplir con sus objetivos de confidencialidad, integridad, autenticación y no repudio.

4. En todo caso, como la protección de la información es una tarea compleja que compete a todos los estados y a todos los estamentos de la sociedad (empresas, instituciones, usuarios, etc.), se hace preciso comenzar a tomar medidas para que, sin importar cuándo la computación cuántica sea una realidad (ya sea a corto/medio/largo plazo), la sociedad en su conjunto esté preparada para asegurar la protección de la información.

5. Es bien sabido que la seguridad de los criptosistemas asimétricos (o de clave pública) más utilizados en la actualidad depende de dos problemas matemáticos considerados computacionalmente difíciles de resolver con los ordenadores disponibles en la actualidad y que podemos considerar como precuánticos.

6. Estos problemas son el problema de la factorización de números enteros (PFE, véase el Anexo A.1), que consiste en determinar los factores primos que dividen a un número entero compuesto dado, y el problema del logaritmo discreto (PLD, véase el Anexo A.2), que requiere determinar la potencia (en el caso de un grupo multiplicativo) a la que se debe elevar el generador dado del grupo considerado, o el múltiplo (en el caso de un grupo aditivo) del generador en el correspondiente grupo.

7. El primero de estos dos problemas es la base de la seguridad del criptosistema RSA [28]; mientras que el segundo lo es, en su versión multiplicativa, del criptosistema de ElGamal [8], y en su versión aditiva, de los criptosistemas basados en curvas elípticas o CCE [15, 19].

8. Como ya se ha mencionado, tanto el PFE como el PLD se han considerado tradicionalmente dos problemas computacionalmente seguros, debido a que la capacidad computacional de los ordenadores actuales requiere de un tiempo de ejecución subexponencial para poder vulnerar (romper) cualquiera de ellos.

9. Sin embargo, Peter Shor en 1997 (sus primeros resultados datan de 1994) publicó dos algoritmos cuánticos capaces de vulnerar ambos problemas de forma eficiente, esto es, en un tiempo de ejecución polinómico, si se dispusiera de un ordenador cuántico con la

suficiente capacidad de cómputo [31]. Tales algoritmos, con los conocimientos actuales, no pueden ser implementados en ordenadores convencionales y requieren para su ejecución de ordenadores cuánticos.

10. Así pues, se puede afirmar que los algoritmos de Shor han demostrado que la criptografía asimétrica de hoy en día es vulnerable a la computación cuántica, por lo que se hace imprescindible la búsqueda y el establecimiento de nuevos sistemas asimétricos que sean invulnerables a este tipo de computación. De hecho, si un ordenador convencional necesita $O\left(2^{\sqrt[3]{\log n}}\right)$ operaciones bit para romper uno de estos dos problemas, un ordenador cuántico, usando el algoritmo de Shor correspondiente, reduciría ese número de operaciones bit a $O(\log^3 n)$ con un almacenamiento de memoria de $O(\log n)$ bits.

11. Debe recordarse que los mismos problemas que sustentan la seguridad de los sistemas de cifrado asimétrico son los que se emplean para garantizar la fiabilidad de los procesos de elaboración y verificación de las firmas electrónicas. Así pues, en términos generales, la seguridad de aquellos es la misma que la de estas.

12. No obstante, en el caso de las firmas, sobre todo cuando se emplean para procesos de autenticación, solo necesitan garantizar su seguridad hasta que son verificadas, lo que suele requerir un periodo de tiempo mucho más corto que el que precisa mantener la confidencialidad de la información. En efecto, si un esquema de firma fuera vulnerado por un ordenador cuántico, es muy probable que el certificado digital con el que se elaboró la misma haya caducado por lo que la seguridad de la firma no se vería comprometida. Caso aparte sería si la validez de la firma fuera de varios años (situación del firmware, por ejemplo).

13. Por su parte, los criptosistemas simétricos (o de clave secreta), hasta la fecha, no parece que sean tan vulnerables a la computación cuántica. Los mejores algoritmos cuánticos que atacan esta criptografía son los algoritmos de Grover [10, 11] y de Simon [32], que reducirían el tiempo de cálculo necesario para romperlos a la raíz cuadrada del tiempo actual. Esto es, si se desarrollara un ordenador cuántico con la capacidad de cómputo suficiente, la seguridad de los sistemas simétricos actuales sería equivalente a la de los mismos sistemas pero con claves cuya longitud fuera la mitad. Es decir, si un ordenador actual necesita de $O(n)$ operaciones bits para romper uno de estos sistemas simétricos, con el algoritmo de Grover este tiempo se reduciría a $O(\sqrt{n})$ operaciones bits y requeriría un almacenamiento en memoria de $O(\log n)$ bits.

14. Hasta ahora no se conoce que exista un ordenador cuántico con la suficiente capacidad de cómputo como para vulnerar los protocolos criptográficos que se emplean en la actualidad y todo apunta a que no se dispondrá de él en breve plazo; sin embargo, con el fin de adelantarse a los acontecimientos futuros que pondrán en peligro los sistemas actuales, el Centro Criptológico Nacional (CCN) publica este documento con el fin de concienciar a los usuarios de la criptografía (organismos y empresas), de la necesidad de ir migrando hacia sistemas criptográficos más robustos y resistentes a la computación cuántica (*quantum resistant*).

15. Debe tenerse en cuenta, además, que para las aplicaciones que manejan información que requiera mantenerse confidencial durante periodos de tiempo largos o con elevados requisitos de seguridad, esta migración hacia nuevos sistemas es una necesidad. Tal necesidad procede del paradigma conocido como «almacena ahora y descifra luego» (*store now, decrypt later*), que podría ser una realidad en el momento en el que se disponga un ordenador cuántico.

2. CRIPTOGRAFÍA POSTCUÁNTICA

16. Debido al desarrollo en la computación cuántica y a su aplicación para vulnerar los sistemas criptográficos precuánticos (usados en la actualidad), desde hace unos años, la comunidad criptográfica ha comenzado a investigar con el fin de proponer nuevos sistemas criptográficos que sean resistentes a tal computación. Esta nueva criptografía, basada en problemas matemáticos diferentes a los empleados en la actualidad (entre los que se encuentran el PFE y el PLD), se ha dado en llamar «criptografía postcuántica» (PQC o *Post-Quantum Cryptography*) o resistente a la computación cuántica.

17. El NIST (*National Institute of Standards and Technology*), como entidad responsable de los procesos de estandarización americanos y debido a la amenaza de la computación cuántica ya comentada, en noviembre de 2016 hizo una Convocatoria Internacional para seleccionar nuevos algoritmos criptográficos resistentes a la computación cuántica con el fin de ser considerados nuevos estándares [22]. El NIST solo incluyó en esta convocatoria a los cifrados asimétricos, los mecanismos de encapsulación de claves o KEM (*Key Encapsulation Mechanism*) y las firmas digitales.

18. La seguridad de los algoritmos presentados a la convocatoria del NIST se ha basado en problemas matemáticos que tienen cabida en las siguientes cinco áreas:

    a) Códigos correctores de errores (criptografía basada en códigos).

    b) Retículos (criptografía basada en retículos).

    c) Funciones resumen (criptografía basada en resúmenes o hashes).

    d) Polinomios multivariantes cuadráticos (criptografía multivariante cuadrática).

    e) Isogenias definidas sobre curvas elípticas (criptografía basada en isogenias).

19. Después de la publicación de los candidatos que han ido superando las diferentes rondas que forman parte del proceso de selección de los candidatos finales, en julio de 2022, el NIST publicó [25, 26] la lista de algoritmos seleccionados (a expensas de una cuarta ronda).

20. Estos candidatos se listan en las Tabla 1 y Tabla 2. En ambas Tablas se indican las áreas a las que pertenecen los candidatos y, entre paréntesis, los correspondientes problemas matemáticos asociados: MLWE (*Module Learning With Errors*, véase el Anexo A.3) y SIS (*Short Integer Solution*, véase el Anexo A.4).

Criptosistema asimétrico y KEM	Área y problema matemático
CRYSTALS-Kyber	Retículo estructurado (MLWE)

Tabla 1. Candidato KEM seleccionado por el NIST después de la tercera ronda y primitiva matemática asociada

Firma digital	Área y problema matemático
CRYSTALS-Dilithium	Retículo estructurado (MLWE)
Falcon	Retículo estructurado (SIS)
SPHINCS$^+$	Funciones hash

Tabla 2. Candidatos a firma seleccionados por el NIST después de la tercera ronda y primitivas matemáticas asociadas

21. El único algoritmo para KEM seleccionado hasta la fecha es CRYSTALS-Kyber [30]; mientras que para firmas se han seleccionado *CRYSTALS-Dilithium* [17], Falcon (*FAst-Fourier Lattice-based COmpact signatures over NTRU*) [27] y SPHINCS+ [12].

22. Como se puede apreciar en las Tabla 1 y Tabla 2, a excepción de la firma digital SPHINCS+, todas las propuestas que han superado la tercera ronda fundamentan su seguridad en el área de retículos. Sin embargo, el proceso de estandarización del NIST no ha terminado, por lo que es posible que nuevas propuestas sean añadidas a las anteriores en un futuro no muy lejano.

23. De hecho, el NIST no ha descartado completamente otras propuestas, de modo que otros cuatro algoritmos continúan para ser analizados en la cuarta ronda. Estos son: BIKE (Bit Flipping Key Encapsulation) [2], HQC (Hamming Quasi-Cyclic) [1], Classic McEliece [3] y SIKE (Supersingular Isogeny Key Encapsulation) [14]. Todos ellos se listan en la Tabla 3.

Criptosistema asimétrico y KEM	Primitiva matemática
BIKE	Códigos de densidad moderada cuasi-cíclicos
HQC	Códigos cuasi-cíclicos de Hamming
Classic McEliece	Códigos de Goppa
SIKE†	Isogenias sobre curvas elípticas
†las últimas investigaciones han mostrado que el algoritmo SIKE es vulnerable, véase el párrafo 26	

Tabla 3. Candidatos a KEM para ser analizados por el NIST en la cuarta ronda y primitivas matemáticas asociadas

24. Tanto BIKE como HQC se basan en códigos estructurados y cualquiera de los dos podría ser considerado adecuado como un KEM de propósito general no basado en retículos. Se cree que el NIST seleccionará uno de estos dos candidatos para la estandarización al final de la cuarta ronda.

25. Por su parte, aunque el Classic McEliece fue propuesto como finalista en la tercera ronda, parece que el NIST no lo está considerando como posible estándar en la actualidad pues, aunque se considera seguro, es probable que no sea muy utilizado debido al gran tamaño de su clave pública.

26. Además, aunque en la fecha de la publicación de los candidatos que habían superado la tercera ronda, SIKE era un candidato atractivo para el NIST por sus menores tamaños de clave y texto cifrado, todo apunta a que no será tenido en cuenta en el futuro, dado que investigadores de la Universidad católica de Lovaina han presentado un trabajo en el que afirman haber encontrado un ataque de recuperación de clave eficiente para SIKEp434 (nivel de seguridad 1) utilizando un procesador de un solo núcleo en, aproximadamente, una hora [5].

27. Por otra parte, para el CCN es de especial importancia el estudio de los algoritmos de acuerdo de clave, por lo que considera, además, del CRYSTALS-Kyber, seleccionado por el NIST y listado en la Tabla 1, el algoritmo basado en retículos no estructurados FrodoKEM [21]. Este algoritmo se puede considerar como una opción conservadora con relación a su seguridad. En la Sección 3.2 se darán más detalles sobre esta recomendación.

28. Finalmente, es importante señalar que el NIST hará una nueva convocatoria para algoritmos de firma digital con firmas cortas y verificación rápida, resistentes a la computación cuántica. Todo apunta a que el NIST busca nuevos esquemas de firma que no se basen en retículos estructurados.

3. RECOMENDACIONES DEL CCN

29. El CCN sigue atentamente las publicaciones del NIST conducentes al establecimiento de nuevos estándares resistentes a la computación cuántica. En este sentido, el CCN, en colaboración con otros organismos internacionales, y especialmente europeos, lleva a cabo sus propias investigaciones sobre los algoritmos postcuánticos propuestos.

30. Ya nadie pone en duda la amenaza que para la criptografía actual supone el desarrollo de los ordenadores cuánticos, por lo que para el CCN es de capital importancia que la comunidad criptográfica española, así como la industria, los organismos y las empresas, comience a prepararse, a la mayor brevedad posible, para evitar o, al menos, paliar, tal amenaza. Para ello es preciso ir adaptándose a los nuevos desarrollos y tener en consideración las propuestas que van superando los diferentes filtros de seguridad. Por este motivo, el CCN recomienda llevar a cabo las acciones necesarias para iniciar los procesos migratorios necesarios para implementar los algoritmos postcuánticos recomendados con el fin de paliar los aspectos adversos de la computación cuántica. Tales recomendaciones se incluyen a continuación.

3.1 PLAN DE MIGRACIÓN

31. Teniendo en cuenta el principio ya mencionado de «almacena ahora y descifra luego», es necesario desarrollar un **plan de migración** que debe incluir los siguientes puntos:

    - Determinar la información que debo proteger y hasta cuándo.
    - Realizar un inventario exhaustivo de productos y cifradores que empleo para proteger mi información y mis activos.
    - Analizar con rigor si tales productos y cifradores son o no resistentes a la computación cuántica.
    - Establecer un plan de migración a los soluciones híbridos (véase la Sección 3.6).
    - Decidir qué nuevos productos necesito y cuánto tiempo requiero para su adquisición y despliegue.
    - Determinar cuánto tiempo tengo disponible (véase el Teorema de Mosca en el ANEXO B).

3.2 MECANISMOS DE ENCAPSULACIÓN DE CLAVES

32. Como ya se ha mencionado anteriormente, el CCN tiene, actualmente, mayor interés en los algoritmos de encapsulación de claves (KEM) que en los de firma. En particular, el CCN no ha abandonado, al igual que otros organismos de seguridad europeos, el algoritmo FrodoKEM, basado en el problema LWE definido sobre retículos, que se incluye en la Tabla 4.

Criptosistema asimétrico y KEM	Primitiva matemática
CRYSTALS-Kyber	Retículo estructurado (MLWE)
FrodoKEM	Retículo no estructurado (LWE)

Tabla 4. Algoritmos KEM recomendados por el CCN y primitivas matemáticas asociadas

33. Debe recordarse que FrodoKEM fue incluido por el NIST en la tercera ronda como un algoritmo alternativo y no como finalista, habiendo sido descartado a partir de la tercera ronda [23].

34. Las razones alegadas por el NIST para su decisión sobre FrodoKEM se deben, fundamentalmente, a que su rendimiento es menor que el de otros algoritmos basados en retículos.

35. Está aceptado que este menor rendimiento se debe a que FrodoKEM no emplea ninguna estructura matemática adicional (solo LWE) al contrario de lo que hacen otros algoritmos basados en retículos, como la definición de una estructura subyacente de anillo (RLWE) o de módulo (MLWE). Esta falta de estructura hace que FrodoKEM sea la opción de seguridad más conservadora, de ahí que el CCN lo mantenga como algoritmo para KEM.

36. Las estructuras adicionales mencionadas (anillo o módulo) ofrecen la ventaja de que los algoritmos que se basan en ellas son más eficientes a la hora de realizar sus cómputos y requieren claves más pequeñas. Sin embargo, la existencia de tal estructura subyacente podría ser la causante de que se desarrollaran ataques contra los algoritmos que las utilizan. De hecho, esta opinión, compartida por algunos organismos de seguridad europeos, parece estar refrendada, de alguna manera, por el propio NIST quien considera a FrodoKEM como una especie de algoritmo de respaldo conservador para el caso en el que se desarrollen ataques contra los algoritmos basados en retículos estructurados.

37. Como es lógico, el CCN también considera como autorizados el KEM seleccionado por el NIST, esto es, el CRYSTAL-Kyber presentado en la Tabla 1, a la vez que tendrá en cuenta el resultado de la cuarta ronda en la que se consideran los KEM mostrados en la Tabla 3, es decir, BIKE, HQC y Classic McEliece.

38. En la Guía de Mecanismos Criptográficos Autorizados del CCN [6] se incluyen, además de otros mecanismos recomendados, el algoritmo antes mencionado, con sus parámetros correspondientes.

3.3 FIRMAS DIGITALES

39. El CCN también recomienda las firmas que el NIST ha seleccionado después de la tercera ronda, es decir, CRYSTALS-Dilithium, Falcon y SPHINCS+. Tales firmas se listan en la Tabla 5.

Firma digital	Primitiva matemática
CRYSTALS-Dilithium	Retículo estructurado (MLWE)
Falcon	Retículo estructurado (SIS)
SPHINCS+	Funciones hash

Tabla 5. Esquemas de firma recomendados por el CCN y primitivas matemáticas asociadas

3.4 FIRMAS BASADAS EN HASH PARA ACTUALIZACIONES DE FIRMWARE

40. Un tipo de algoritmo que no se ha considerado en la convocatoria del NIST son los métodos de firma digital basados en funciones hash con estado. Probablemente el hecho se justifique porque la seguridad ofrecida por estos algoritmos ha sido largamente estudiada y se considera que son seguros ante la computación cuántica. No obstante, es sabido que, aunque presentan algunas desventajas, como que solo se pueden realizar un número limitado de firmas, son especialmente adecuados para firmar actualizaciones de firmware, dado que su duración es mayor que la de las firmas habituales y que el número de firmas a generar, dada una clave, es limitado.

41. Tales algoritmos son los conocidos como firma de *Leighton-Micali* o LMS (Leighton-Micali Signature) [18] y esquema de firma de Merkle extendida o XMSS (*eXtended Merkle Signature Scheme*) [4, 13] y han sido estandarizados por el IETF (Internet Engineering Task Force). También el NIST dio a conocer la Publicación Especial SP800-208 en la que adopta estos estándares [24].

42. El CCN recomienda el **uso de forma inmediata del esquema XMSS para la actualización de firmware**, tal y como se muestra en la Tabla 6.

Firma para firmware	Primitiva matemática
XMSS	Funciones hash con estado

Tabla 6. Esquema de firma para firmware recomendado por el CCN y primitiva matemática asociada

3.5 LONGITUDES DE CLAVE PARA ALGORITMOS SIMÉTRICOS Y FUNCIONES HASHES

43. Como ya se mencionó en la Sección 1. , los algoritmos de cifrado simétrico se consideran menos vulnerables a la computación cuántica que los asimétricos, dado que la amenaza demostrada hasta ahora es que, caso de existir un ordenador cuántico con la suficiente capacidad de cómputo, la seguridad que ofrecen sería equivalente a la del mismo algoritmo cuya clave tuviera la mitad de la longitud original.

44. Por este motivo, solo se recomienda el uso de algoritmos con claves de, al menos, 256 bits, dado que tal seguridad, en presencia de un ordenador cuántico, sería equivalente a la del mismo algoritmo con una clave de 128 bits que, a día de hoy, se considera aceptable.

45. Así pues, se recomienda utilizar algoritmos simétricos, tipo AES, con claves de 256 bits y especialmente en aquellos casos en los que la protección de la información sea importante.

46. De forma análoga, no se recomienda el uso de funciones hash que proporcionen resúmenes de menos de 256 bits. Por ello, las funciones hash recomendadas son las de las familias SHA2 y SHA3 con resúmenes mayores a 256 bits.

47. En la Tabla 7 se listan los algoritmos simétricos y las funciones hashes recomendadas por el CCN.

Algoritmo	Longitud de clave/resumen
AES	256
SHA2	256 384 512
SHA3	256 384 512

Tabla 7. Algoritmos simétricos recomendados por el CCN y las longitudes de clave o resúmenes correspondientes

3.6 SOLUCIONES HÍBRIDAS

48. Dado que los algoritmos criptográficos postcuánticos en proceso de estandarización son relativamente nuevos, es claro que necesitarán de un largo periodo de análisis para garantizar su seguridad. Además, en los últimos años se han venido publicando ataques contra los mismos, que explotan, fundamentalmente, errores en sus implementaciones y ataques por canal lateral o inducción de fallos. Por estas razones se debe considerar la recomendación de emplear soluciones híbridas, es decir, combinar de modo simultáneo algoritmos postcuánticos con algoritmos precuánticos.

49. Dicho de otro modo, una «solución híbrida» consiste en construir una solución que combine primitivas precuánticas (actuales) y primitivas postcuánticas, con el fin de obtener tanto las garantías criptográficas tradicionales como las que ofrecen las soluciones resistentes a la computación cuántica [16].

50. Otra ventaja adicional de las soluciones híbridas es que facilitan el desarrollo de soluciones cripto-ágiles (ver Sección 3.7). En efecto, si uno de los algoritmos de la solución resultara ser vulnerable, sería fácilmente reemplazable por otro de su misma familia.

51. Por otra parte, es claro que la hibridación no es una solución permanente. De hecho, se trata de paso intermedio en la migración de la criptografía actual a la postcuántica, dado que a medida que vaya pasando el tiempo, la PQC se irá convirtiendo en una solución cada vez más confiable.

52. A modo de ejemplo, se puede mencionar que en los mecanismos de encapsulación de claves, las salidas de ambos algoritmos se envían a una función de derivación de claves (KDF o *Key Derivation Function*) para producir la clave para el cifrado simétrico (véase la Figura 1).

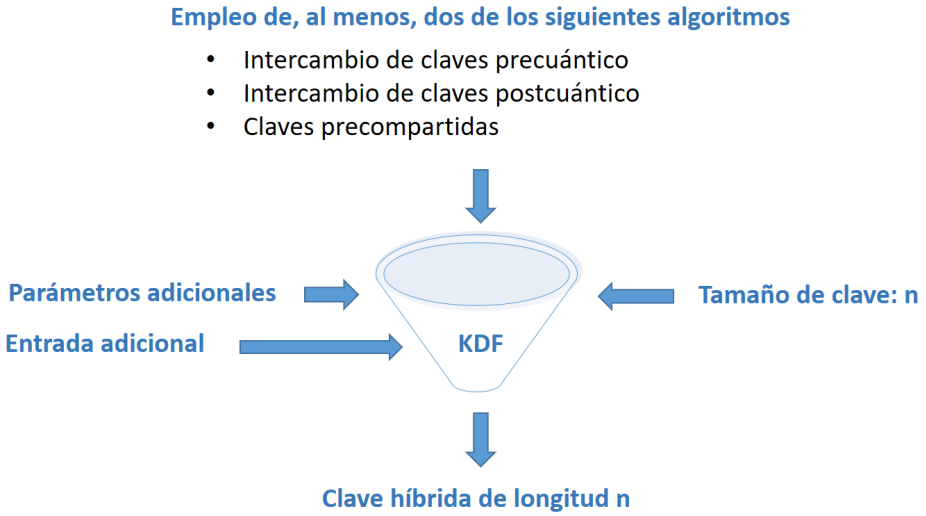


Figura 1. Solución híbrida para el intercambio de claves como medida de transición

53. Además, el empleo de soluciones híbridas requiere, en ocasiones, ajustar los protocolos criptográficos utilizados actualmente. De hecho ya existen recomendaciones en este sentido para los protocolos TLS (Transport Layer Security) [33] e IKEv2 (Internet Key Exchange) [9, 34].

54. El CCN recomienda el **uso de soluciones híbridas tan pronto como sea posible**.

3.7 CRIPTO-AGILIDAD

55. El concepto de «cripto-agilidad» o agilidad criptográfica es la capacidad que debe tener un sistema de seguridad para cambiar de forma rápida a nuevos mecanismos de cifrado ante la aparición de vulnerabilidades o amenazas contra los algoritmos empleados de forma habitual por dicho sistema.

56. La idea subyacente a este concepto es la de la rápida adaptación a nuevos estándares criptográficos de modo que ello no suponga cambios importantes en la infraestructura utilizada. Debe tenerse en cuenta que este cambio puede llevar consigo decisiones de calado. Si se presenta una situación como la señalada, una organización debe poder cambiar rápidamente a un método de cifrado diferente para minimizar el daño. Este proceso incluye cambiar algoritmos criptográficos, claves de seguridad, certificados y otras tecnologías criptográficas.

57. Así pues, la cripto-agilidad no solo fomenta el desarrollo y la evolución del sistema, sino que también actúa como medida de seguridad o mecanismo de respuesta a incidentes.

58. Es posible que se publiquen nuevos ataques contra los sistemas criptográficos empleados actualmente así como que se disponga de un ordenador cuántico con la suficiente capacidad de cómputo como para romper los criptosistemas actuales. Es por ello que la cripto-agilidad cobra mayor importancia y hay que poner especial atención a los mecanismos criptográficos empleados, de modo que sean lo suficientemente flexibles para que permitan reaccionar con rapidez y paliar las amenazas de los nuevos desarrollos y que posibiliten garantizar el nivel de seguridad necesario.

59. En definitiva, la cripto-agilidad debería convertirse en un criterio de diseño para nuevos productos, al margen del estado de desarrollo de los ordenadores cuánticos.

3.8 CALENDARIO RECOMENDADO

60. A la vista de los comentarios anteriores, parece oportuno establecer un calendario para llevar a cabo las acciones recomendadas de modo que el paso de la criptografía precuántica a la postcuántica se lleve a cabo siguiendo una transición gradual.

61. El calendario recomendado deberá seguir las siguientes fases:

FASE 1	• Empleo inmediato de las firmas basadas en hash para actualizaciones de firmware.
FASE 2	• Uso de soluciones híbridas para proporcionar mayor defensa a la criptografía precuántica
FASE 3	• Empleo de soluciones híbridas con las garantías de seguridad proporcionadas por la criptografía postcuántica.
FASE 4	• Adopción de los algoritmos criptográficos postcuánticos considerados resistentes a la computación cuántica.

62. De forma más precisa, las acciones de cada una de las fases son las siguientes:

- **Fase 1**: Tal y como se ha comentado en la Sección 3.4, el CCN recomienda el uso de forma inmediata del esquema XMSS para la actualización de firmware (véase la Tabla 6).
- **Fase 2**: En la Sección 3.6 se ha señalado la importancia de utilizar soluciones híbridas para combinar las primitivas precuánticas con las primitivas postcuánticas, con el fin de obtener las garantías probadas de seguridad que ofrecen las primeras a las que se añadirían las que ofrecen las segundas. Estas garantías estarían alineadas con las ventajas de la cripto-agilidad comentadas en la Sección 3.7. Esta segunda fase debería iniciarse a la mayor brevedad posible, haciendo uso de los algoritmos recomendados por el CCN y mencionados en este documento, ya sean KEM (véase la Tabla 4), firma digital (véase la Tabla 5), firmas basadas en hash para actualizaciones de firmware (véase la Tabla 6) o simétricos (véase la Tabla 7). Se prevé que esta fase dure hasta 2025.
- **Fase 3**: Se potenciará el proceso de hibridación de modo que a los algoritmos seguros de la criptografía precuántica se unan los algoritmos postcuánticos recomendados por el CCN. En este sentido, es probable que se afiancen los algoritmos ya comentados en la Fase 2, a la vez que se puedan considerar algunos de los algoritmos que están siendo analizados en la cuarta fase convocada por el NIST (véase la Tabla 3). Esta fase debería dar comienzo en 2025 y durar, al menos, hasta 2030.
- **Fase 4**: En esta fase se deberían adoptar e implementar de forma generalizada los algoritmos que hayan sido recomendados por el CCN; abandonando, en la medida de lo posible, las soluciones híbridas. Es probable que esta fase no se pueda iniciar antes de 2030.

63. En la Figura 2 se muestra el calendario que se recomienda para implementar las fases anteriormente señaladas.

Figura 2. Calendario de actuación recomendado para la transición de la criptografía precuántica a la postcuántica

4. REFERENCIAS

[1] C. Aguilar Melchor, N. Aragon, S. Bettaieb, L. Bidoux, O.Blazy, J.C. Deneuville, P. Gaborit, E. Persichetti, G. Zémor, and J. Bos. HQC (Hamming Quasi-Cyclic). NIST, Round 2, 2020. http://pqc-hqc.org/index.html.

[2] N. Aragon, P. Barreto, S. Bettaieb, L. Bidoux, O. Blazy, J.C. Deneuville, P. Gaborit, S. Gueron, T. Guneysu, C. Aguilar Melchor, R. Misoczki,E. Persichetti, N. Sendrier, J.P. Tillich, G.Zemor, and V. Vasseur. *BIKE (Bit Flipping Key Encapsulation)*. NIST, Round 2, 2020. https://bikesuite.org/files/v4.0/BIKE_Spec.2020.05.03.1.pdf.

[3] D.J. Bernstein, T. Chou, T. Lange, I. von Maurich R. Misoczki, R. Niederhagen, E. Persichetti, C. Peters, P. Schwabe, N. Sendrier, J. Szefer,and W. Wang. *Classic McEliece*. NIST, Round 2, 2020. https://classic. mceliece.org/.

[4] J. Buchmann, E. Dahmen, and A. Hülsing. XMSS - a practical forward secure signature scheme based on minimal security assumptions. In *Proc. Post-Quantum Cryptography (PQCrypto 2011), Lecture Notes Comput. Sci.*, volume 7071, pages 117–129, 2011. https://doi.org/10.1007/ 978-3-642-25405-5_8.

[5] W. Castryck and T. Decru. An efficient key recovery attack on SIDH (preliminary version). *Cryptology ePrint Archive, Report 2022/975*, 2022. https://eprint.iacr.org/2022/975.

[6] CCN. *Guía de Mecanismos Criptográficos Autorizados*. Centro Criptológico Nacional, 2022. (pendiente de publicación).

[7] R. Durán Díaz, L. Hernández Encinas, and J. Muñoz Masqué. *El criptosistema RSA*. RA-MA, Madrid, España, 2005. https://www.ra-ma.es/libro/ el-criptosistema-rsa_141831/.

[8] T. ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Trans. Inform. Theory*, 31:469–472, 1985. https://doi.org/10.1109/TIT.1985.1057074.

[9] S. Fluhrer, P. Kampanakis, D. McGrew, and V. Smyslov. *Mixing Preshared Keys in the Internet Key Exchange Protocol Version 2 (IKEv2) for Post-quantum Security*. Internet Engineering Task Force, RFC 8784, 2020. https://tools.ietf.org/html/rfc8784.

[10] L.K. Grover. A fast quantum mechanical algorithm for database search. In *Proc. 28th annual ACM symposium on Theory of Computing (STOC'96)*, pages 212–219, 1996. https://doi.org/10.1145/800070.802214.

[11] L.K. Grover. Quantum mechanics helps in searching for a needle in a haystack. *Phys. Rev. Lett.*, 79(2):325–328, 1997. https://doi.org/10.1103/PhysRevLett.79.325.

[12] A. Hulsing, D.J. Bernstein, C. Dobraunig, M. Eichlseder, S. Fluhrer, S.-L.Gazdag, P. Kampanakis, S. Kolbl, T. Lange, M.M. Lauridsen, F. Mendel,R. Niederhagen, C. Rechberger, J. Rijneveld, P. Schwabe, and J.-P. Aumasson.SPHINCS+. Online

publication, 2020. https://sphincs.org/.

[13] A. Hülsing, D. Butin, S.L. Gazdag, J. Rijneveld, and A. Mohaisen. *XMSS: extended Merkle signature scheme*. Internet Engineering Task Force, RFC 8391, 2018. https://tools.ietf.org/html/rfc8391.

[14] D. Jao, R. Azarderakhsh, M. Campagna, C. Costello, L. De Feo, B. Hess, A. Jalali, B. Koziel, B. LaMacchia, P. Longa, M. Naehrig, J. Renes, V. Soukharev, and D. Urbanik. SIKE: Supersingular Isogeny Key Encapsulation,2016. http://sike.org.

[15] N. Koblitz. Elliptic curve cryptosytems. *Math. Comp.*, 48(177):203–209, 1987. https://doi.org/10.1090/S0025-5718-1987-0866109-5.

[16] B.A. LaMacchia. *Getting Ready for the Post-Quantum Transition*. Microsoft Utimaco Webinar, 2020. https://ecstech.com/wp-content/uploads/2020/08/2020_ISO_BLaMacchia_Final.pdf.

[17] V. Lyubashevsky, L. Ducas, E. Kiltz, T. Lepoint, P. Schwabe, G. Seiler, andD. Stehle. CRYSTALS-DILITHIUM. Online publication, 2020. https:// pq-crystals.org/.

[18] D. McGrew, M. Curcio, and S. Fluhrer. *Leighton-Micali hash-based signatures*. Internet Engineering Task Force, RFC 8554, 2019. https://tools.ietf.org/html/rfc8554.

[19] V.S. Miller. Use of elliptic curves in cryptography. *Lecture Notes Comput. Sci.*, 218:417–426, 1986. https://doi.org/10.1007/3-540-39799-X_31.

[20] M. Mosca. *Cybersecurity in a Quantum World: will we be ready?* Universtiyof Waterloo, 2015. https://csrc.nist.gov/csrc/media/events/ workshop-on-cybersecurity-in-a-post-quantum-world/documents/ presentations/session8-mosca-michele.pdf.

[21] M. Naehrig, E. Alkim, J. Bos, L. Ducas, K. Easterbrook, B. LaMacchia,P. Longa, I. Mironov, V. Nikolaenko, C. Peikert, A. Raghunathan, and D. Stebila. FrodoKEM. Online publication, 2020. https://frodokem.org/.

[22] NIST. Post-quantum cryptography. On-line publication, 2017. https:// csrc.nist.gov/Projects/Post-Quantum-Cryptography.

[23] NIST. PQC standardization process: Third round candidate announcement. Online publication, 2020. https://csrc.nist.gov/News/2020/ pqc-third-round-candidate-announcement.

[24] NIST. *Recommendation for Stateful Hash-Based Signature Schemes*. National Institute of Standard and Technology, Special Publication, SP800-208, 2020. https://doi.org/10.6028/NIST.SP.800-208.

[25] NIST. Post-quantum cryptography. selected algorithms 2022. On-line publication, 2022. https://csrc.nist.gov/Projects/ post-quantum-cryptography/selected-algorithms-2022.

[26] NIST. PQC standardization process: Announcing four candidates to be standardized, plus fourth round candidates. Online publication, 2022. https://csrc.nist.gov/News/2022/ pqc-candidates-to-be-standardized-and-round-4.

[27] T. Prest, P.A. Fouque, J. Hoffstein, P. Kirchner, V. Lyubashevsky, T. Pornin, T. Ricosset, G. Seiler, W. Whyte, and Z. Zhang. Falcon. Online publication, 2020. https://falcon-sign.info/.

[28] R. Rivest, A. Shamir, and L.M. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM*, 21(2):120–126, 1978. https://doi.org/10.1145/359340.359342.

[29] A. Fúster Sabater, L. Hernández Encinas, A. Martín Muñoz, F. Montoya Vitini, and J. Muñoz Mas qué. *Criptografía, protección de datos y aplicaciones. Guía para estudiantes y profesionales*. RA-MA, Madrid, España, 2012. https://www.ra-ma.es/libro/ criptografia-proteccion-de-datos-y-aplicaciones-una-guia-para\-estudiantes-y-profesionales_48492/.

[30] P. Schwabe, R. Avanzi, J. Bos, L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, J.M. Schanck, G.Seiler, and D. Stehle. CRYSTALS-KYBER. Online publication, 2020. https://pq-crystals.org/.

[31] P.W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5):1484–1509, 1997. https://doi.org/10.1137/S0097539795293172.

[32] D.R. Simon. On the power of quantum computation. *SIAM Journalon Computing*, 26(5):1474–1483, 1997. https://doi.org/10.1137/S0097539796298637.

[33] D. Stebila, S. Fluhrer, and S. Gueron. *Hybrid key Exchange in TLS 1.3 (draft-ietf-tls-hybrid-design-04).* Internet Engineering Task Force, RFC 7296. https://tools.ietf.org/html/ draft-stebila-tls-hybrid-design-03, year = 2020.

[34] C. Tjhai, M. Tomlinson, G. Bartlett, S. Fluhrer, D. Van Geest, O. Garcia-Morchon, and V. Smyslov. *Multiple Key Exchanges in IKEv2 (draft-ietf-ipsecme-ikev2-multiple-ke-08)*. Internet Engineering Task Force, RFC 7296, 2023. https://datatracker.ietf.org/doc/pdf/ draft-ietf-ipsecme-ikev2-multiple-ke-08.

ANEXO A. PROBLEMAS MATEMÁTICOS

64. En este anexo se presentan las definiciones de los problemas matemáticos en los que se fundamenta la seguridad de determinados criptosistemas mencionados en este documento, así como otros aspectos matemáticos que se consideran oportunos para la comodidad del lector.

A.1. PROBLEMA DE LA FACTORIZACIÓN DE NÚMEROS ENTEROS (PFE)

65. El problema matemático en el que se fundamenta la seguridad de uno de los criptosistemas de clave pública más utilizados en la actualidad (RSA) es el problema de la factorización de números enteros [7, 29].

66. Es conocido el **Teorema Fundamental de la Aritmética**, en el que se afirma que todo número compuesto n ≥ 2 admite una factorización única como producto de potencias de primos:

$$n = \prod_{i=1}^{k} p_i^{e_i} = p_1^{e_1} \bullet p_2^{e_2} \bullet \ldots \bullet p_k^{e_k}$$

67. siendo los p_i primos distintos y cada e_i un entero positivo. A partir de este teorema se plantea el siguiente problema.

> **Definición 1**
> El «**problema de la factorización**» de un número entero compuesto n consiste en determinar su factorización como producto de sus factores primos.

68. Los métodos de factorización se clasifican en dos grupos dependiendo, fundamentalmente, de su tiempo de ejecución: los de «propósito general» y los de «propósito especial». Los tiempos de computación de los de propósito general sólo dependen del tamaño del número compuesto a factorizar; mientras que los segundos proporcionan mejores resultados, es decir, su tiempo de computación mejora si el número a factorizar tiene propiedades especiales.

69. En el grupo de los métodos de propósito general están el método de la criba cuadrática y el de la criba general del cuerpo numérico; mientras que en el grupo de los de propósito especial destacan el método de las divisiones sucesivas, los métodos $\rho(ro)$ y $p-1$ de Pollard, el método de las curvas elípticas y el método de la criba especial del cuerpo de números.

70. Como norma, en el problema de la factorización de un número compuesto se deben utilizar, en primer lugar, los métodos de propósito especial dado que suelen ser más eficientes. Por esta razón, inicialmente se deben buscar los factores primos pequeños del número compuesto dado utilizando, siempre que sea posible, algunas de las propiedades del número. Si estos métodos no proporcionan la solución deseada, se pueden utilizar los métodos de propósito general.

A.2. PROBLEMA DEL LOGARITMO DISCRETO (PLD)

71. El «problema del logaritmo discreto» es un caso particular del problema general del cálculo de logaritmos. Es conocido que el logaritmo de a en la base b es el número $x \in \mathbb{R}$, escrito, $log_b a = x$, precisamente si x es la potencia a la que hay que elevar la base para obtener el número dado: $b^x = a$

72. No obstante, cuando el conjunto de los números reales se sustituye por el grupo multiplicativo $\mathbb{Z}_p^*$, entonces se habla del logaritmo discreto [7, 29]. De forma más precisa,

> **Definición 2** Dado un número primo p, un generador g del grupo cíclico multiplicativo $\mathbb{Z}_p^*$ y un elemento $a \in \mathbb{Z}_p^*$, el ***problema del logaritmo discreto*** consiste en determinar de forma eficiente el entero $x\ con\ 0 \leq x \leq p-2$ de modo que $g^x \equiv a\ (mod\ p)$, es decir, $x = log_g a (mod\ p)$.

73. Si el grupo cíclico es aditivo, todo elemento del grupo G será un múltiplo del generador g, $g + g + \cdots + g = k \cdot g$. Por tanto, en este caso se tiene la siguiente

> **Definición 3** Dado un grupo aditivo cíclico G, un elemento $a \in G$ y un generador g, el ***problema del logaritmo elíptico*** (a veces llamado logaritmo discreto aditivo) consiste en determinar de forma eficiente el entero $x\ con\ 0 \leq x \leq p-2$ de modo que $x \cdot g = a$.

74. El problema del logaritmo discreto es el problema en el que se basa la seguridad de determinados protocolos criptográficos, como es el protocolo de cambio de clave de Diffie-Hellman (DH) y el esquema de cifrado de ElGamal. Por su parte, el problema del logaritmo elíptico es la base de la seguridad del protocolo análogo de cambio de clave de Diffie-Hellman sobre curvas elípticas (ECDH) y los esquemas de cifrado basados en curvas elípticas (ECC).

A.3. PROBLEMA DEL APRENDIZAJE CON ERRORES (LWE)

75. El problema del aprendizaje con errores (LWE o Learning With Errors) se parametriza por un entero n, un número primo $q \geq 2$ y una distribución de probabilidad $\chi\ sobre\ \mathbb{Z}_q$.

76. Típicamente χ es una distribución normal de media v y desviación estándar δ:

$$\chi = G(x) = \frac{1}{\delta\sqrt{2\pi}} exp^{\frac{1}{2}\left(\frac{x-v}{\delta}\right)^2}$$

77. Una distribución $A_{s,\chi}$ de un problema LWE sobre $\mathbb{Z}_q^n \times \mathbb{Z}_q$ se muestrea eligiendo uniforme y aleatoriamente $a \xleftarrow{\chi} \mathbb{Z}_q^n,\quad e \xleftarrow{\chi} \mathbb{Z}_q$ y considerando como salida el par $(\boldsymbol{a}, b), siendo\ b = \langle s, \boldsymbol{a} \rangle + e\ (mod\ q)$

78. Existen dos versiones del problema LWE: búsqueda y decisión.

79. En la **versión de búsqueda del problema LWE** se dan m muestras independientes $(\boldsymbol{a}_i, b_i) \in \mathbb{Z}_q^n \times \mathbb{Z}_q\ de A_{s,\chi}\ con\ b_i = \langle s, \boldsymbol{a}_i \rangle + e_i\ (mod\ q) \in \mathbb{Z}_q$ y se trata de encontrar el vector secreto $s \in \mathbb{Z}_q^n\ siendo\ m > n$.

80. La idea es determinar el valor s a partir de m muestras dadas:

$$a_1 \xleftarrow{\chi} \mathbb{Z}_q^n,\quad b_1 = \langle s, a_1 \rangle + e_1\ (mod\ q)$$

$$a_2 \xleftarrow{\chi} \mathbb{Z}_q^n,\quad b_2 = \langle s, a_2 \rangle + e_2\ (mod\ q)$$

$$\vdots$$

$$a_m \xleftarrow{\chi} \mathbb{Z}_q^n,\quad b_m = \langle s, a_m \rangle + e_m\ (mod\ q)$$

81. En la **versión de decisión del problema LWE**, el objetivo es distinguir entre dos pares de vectores

$$(a_i, b_i) \; y \; (\overline{a_\iota}, \overline{b_\iota}) \; donde \; a_i, \overline{a_\iota} \underset{\chi}{\leftarrow} \mathbb{Z}_q^n, \; b_i = \langle s, \boldsymbol{a}_i \rangle + e_i \; (mod \; q) \epsilon \, \mathbb{Z}_q \; y \; \overline{b_\iota} \; \epsilon \, \mathbb{Z}_q$$

Es decir, se trata de decidir, para un par de vectores dados, si el segundo vector es el producto escalar del primer vector por algún vector secreto, s sumado con algún error, o si es el segundo vector es uniformemente aleatorio.

82. En el caso de que se considere una estructura subyacente de anillo en el retículo, se habla del problema LWE sobre anillos (RLWE o Ring Learning With Errors) y si tal estructura es la de módulo, se habla del problema LWE sobre módulos o MLWE (*Module Learning With Errors*)

A.4. PROBLEMA DE LA SOLUCIÓN ENTERA MÁS CORTA (SIS)

83. En el problema de la solución entera más corta o SIS (*Short Integer Solution*) se consideran m vectores uniformemente aleatorios $a_i \in \mathbb{Z}_q^n$ que definen una matriz $A \in \mathbb{Z}_q^{n \times m}$ y se trata de encontrar un vector no nulo $z \in \mathbb{Z}^m de \; norma \; \| z \| \leq \varepsilon$ tal que:

$$A \cdot z = \sum_{i=1}^{m} a_i z_i = 0 \; \in \mathbb{Z}_q^n$$

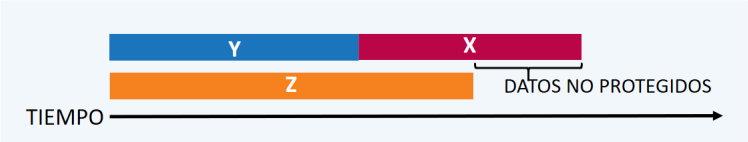
ANEXO B. TEOREMA DE MICHELE MOSCA

84. El teorema de Mosca puede enunciarse en los siguientes términos [20]:

85. **Teorema** Sea x el tiempo (en años) que uno necesita que sus datos confidenciales sean seguros, y el tiempo (en años) que uno necesita para volver a equipar la infraestructura existente con una solución resistente a la computación cuántica (QR) y z el tiempo (en años) que se tardará en construir un ordenador cuántico a gran escala (o cualquier otro avance relevante). Entonces, si $x + y > z$, uno tiene un grave problema.

TEOREMA DE MOSCA

- Si x + y > z , tenemos un problema.



- X tiempo que deseamos que nuestros datos estén seguros.
- Y tiempo que llevará migrar nuestros sistemas a QR.
- Z tiempo que tardaran los ordenadores cuánticos en vulnerar nuestros sistemas.

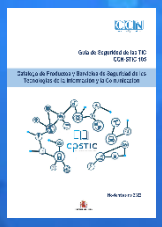
Figura 3. Esquema gráfico del teorema de mosca

CCN-PyTec
centro criptológico nacional

El Departamento de Productos y Tecnologías de Seguridad TIC del Centro Criptológico Nacional (CCN-PyTec) promueve el desarrollo, la evaluación, la certificación y el uso de productos para garantizar la seguridad de los sistemas de tecnologías de la información y la comunicación.

CPSTIC
CATÁLOGO DE PRODUCTOS Y SERVICIOS STIC

CATÁLOGO DE PRODUCTOS Y SERVICIOS DE SEGURIDAD TIC



PDF

ONLINE

ccn-pytec@cni.es

@CCNPYTEC

CCN-PYTEC

www.ccn.cni.es **https://oc.ccn.cni.es** **www.ccn-cert.cni.es**