eurecat

"innovating for business"

Preparant-nos per l'era quàntica... amb la criptografia postquàntica.

Dr. Juan Caubet
Director de la Unidad de IT&OT Security
juan.caubet@eurecat.org
@juancaubet

www.eurecat.org

COMPUTACIÓN CUÁNTICA Y CIBERSEGURIDAD

Purpose	Meaning	Cryptography required
Secrecy/Confidentiality	Only sender and receiver can read (= decrypt) the message, and no one else can.	Symmetric encryption
Authentication	Receiver can firmly establish that the message comes from sender.	
Integrity	The message is unaltered	
Non-repudiation	Sender cannot deny having sent the message.	Public-key signatures

Seguridad Computacional

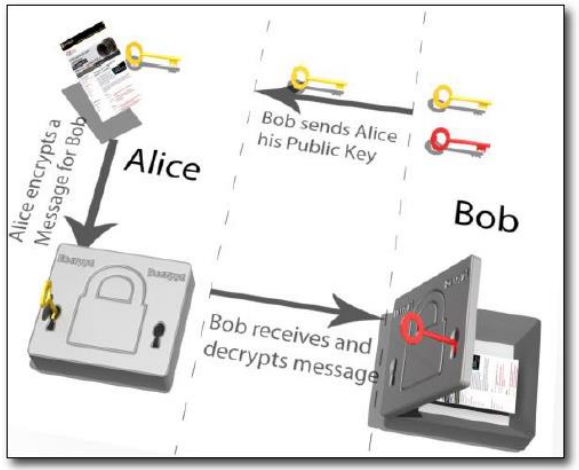
HSD
The Hague Security Delta

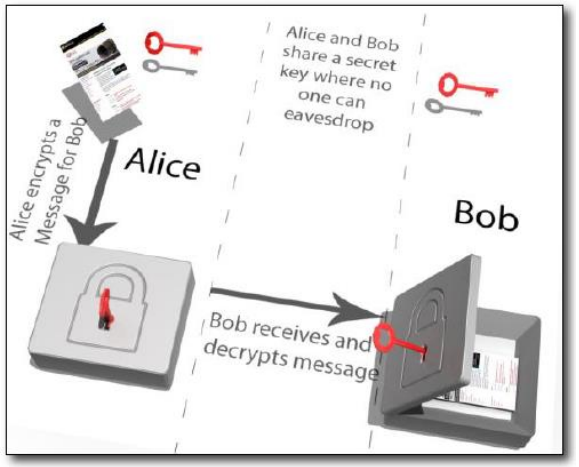
CRIPTOGRAFÍA ACTUAL

- Todos los **sistemas criptográficos de cifrado** dan como resultado una **clave criptográfica de cifrado**, normalmente una larga cadena de números, que se utiliza para **transformar la información** que se desea cifrar.

- Uno de los sistema de cifrado más utilizados es el **RSA**, que basa su seguridad en el problema matemático de **descomposición de números enteros en factores primos**.

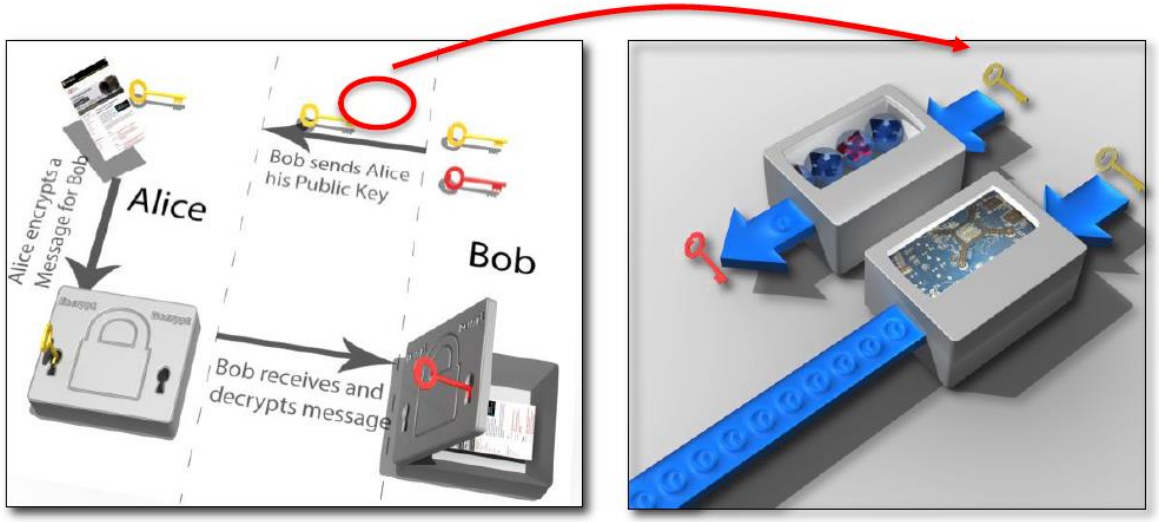
- Estos sistemas de cifrado son utilizados en **conexiones VPNs, conexiones HTTP seguras, firmas digitales, etc.**





ATAQUE CUÁNTICO

- Los **algoritmos criptográficos asimétricos**, como el RSA, utilizados en los protocolos de intercambio de claves o firma digital, parecen ser **los más vulnerables** a ser comprometidos por parte de algoritmos cuánticos conocidos, concretamente por parte del **algoritmo de Shor**.



¿QUÉ ES LA CRIPTOGRAFÍA POSTCUÁNTICA?

- Es sabido que los **protocolos de comunicación actuales son altamente vulnerables a ataques cuánticos**:
  - Cualquier sistema criptográfico que base su seguridad en los problemas matemáticos *Integer Factorization* y *Discrete Logarithm*, tales como RSA, DSA, DH, ECDH, ECDSA y otras variantes, es vulnerable a un ataque cuántico.
- Los **algoritmos criptográficos postcuánticos son resistentes a ataques cuánticos**:
  - Los algoritmos criptográficos postcuánticos basan su seguridad en **otros problemas matemáticos**, difíciles de solucionar también para ordenadores cuánticos.
  - Cualquier sistema criptográfico postcuántico debe poder ser ejecutado en un **ordenador convencional**.

¿QUÉ ES LA CRIPTOGRAFÍA POSTCUÁNTICA?

Técnicas matemáticas más utilizadas

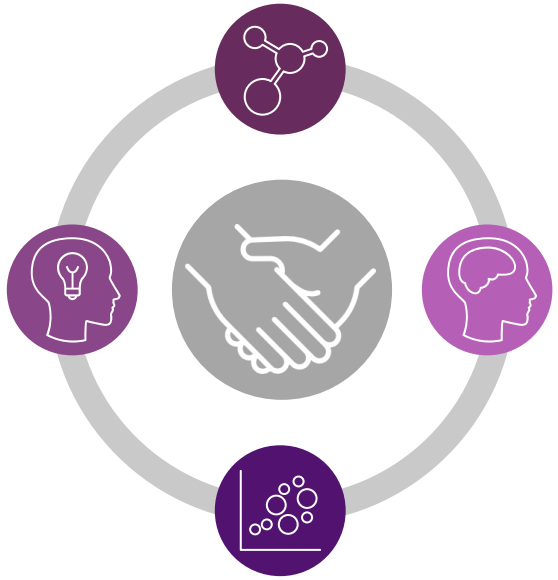
Retículos

Se pueden entender como una red de puntos distribuidos de forma regular en el plano.

Problemas del vector más corto o el más cercano.

Códigos algebraicos

Aquí el problema subyacente es el de decodificar una palabra codificada a través de un código lineal desconocido.



Isogenias de CE

La seguridad de sus algoritmos se basa en el cálculo explícito de isogenias entre curvas, así como en el cálculo de ciertos conjuntos de isogenias.

Polinomios multivariable

Los problemas están asociados a la resolución de sistemas de ecuaciones no lineales en varias variables sobre cuerpos finitos.

Utilizados para esquemas de firma digital.

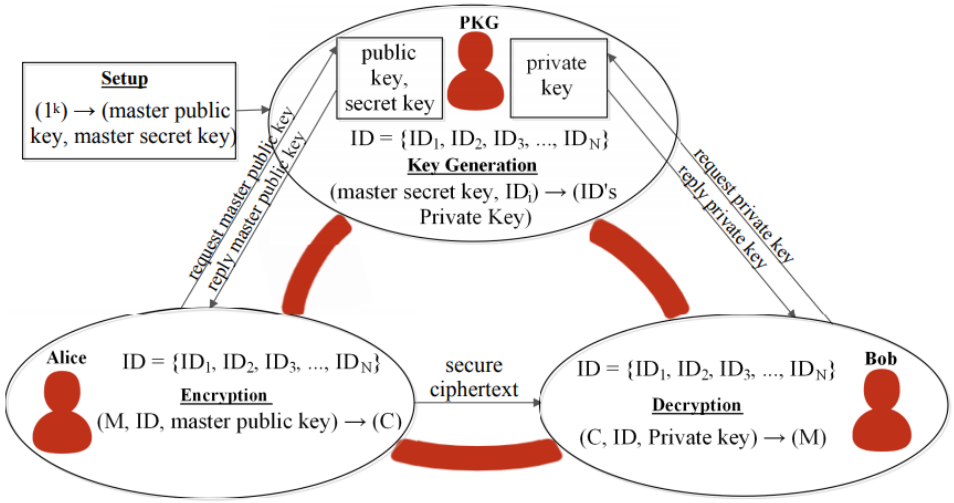
¿QUÉ ES LA CRIPTOGRAFÍA POSTCUÁNTICA?

Identity-based Public Key Cryptography (IDPKC)

- Se trata de **sistemas criptográficos basados en la identidad** de los usuarios o dispositivos cuya seguridad cuántica apenas se ha empezado a explorar.

- Uno de sus principales objetivos es **evitar el uso de certificados digitales** para generar confianza en las claves públicas.

- Su ventaja es que simplemente utiliza la **identidad conocida del destinatario para obtener la clave pública**.



NIST PQC Standarization Challenge

01 Recepción de iniciativas.

02 Seleccionadas 26 propuestas.

03 Seleccionadas 7 propuestas.

04 Selec. propuestas ganadoras.

NIST
National Institute of Standards and Technology

La situación en Europa

Network Working Group
Internet-Draft
Intended status: Informational
Expires: August 15, 2020

D. Stebila
University of Waterloo
S. Fluhrer
Cisco Systems
S. Gueron
U. Haifa, Amazon Web Services
February 12, 2020

Hybrid key exchange in TLS 1.3
draft-stebila-tls-hybrid-design-03

Abstract

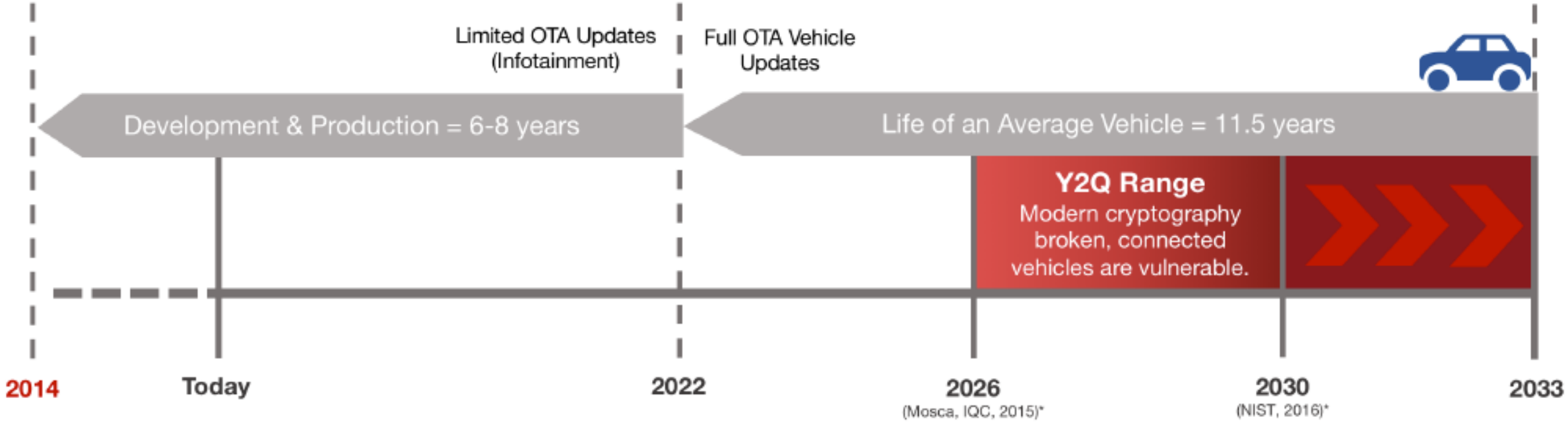
Hybrid key exchange refers to using multiple key exchange algorithms simultaneously and combining the result with the goal of providing security even if all but one of the component algorithms is broken. It is motivated by transition to post-quantum cryptography. This document provides a construction for hybrid key exchange in the Transport Layer Security (TLS) protocol version 1.3.

Discussion of this work is encouraged to happen on the TLS IETF mailing list tls@ietf.org or on the GitHub repository which contains the draft: https://github.com/dstebila/draft-stebila-tls-hybrid-design.

ETSI TR 103 619 V1.1.1 (2020-07)

CYBER;
Migration strategies and recommendations to Quantum Safe schemes

¿CUÁNDO DEBERÍAMOS TENER DESPLEGADO UN SISTEMA QUANTUM-SAFE?



¿QUÉ HACEMOS EN EURECAT?

1

Investigación

Trabajamos principalmente sobre teoría de retículos e isogenias de curvas elípticas super-singulares en firma digital.

2

Implementación

Hemos implementado una serie de algoritmos postcuánticos que cubren los escenarios criptográficos más importantes: cifrado y descifrado, firma digital e intercambio de claves.

3

Testeo

Estamos trabajando en la integración de un algoritmo de firma digital en una Blockchain y en el uso de algoritmos postcuánticos en dispositivos IoT.

+

Universitat de Lleida

UPC

Entanglement Partners_ >

Colaboraciones

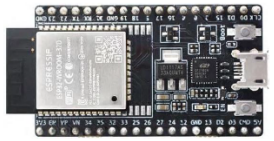
Colaboración con la UPC en la co-supervisión de una tesis doctoral, con la UdL en la implementación y testeo de algoritmos en dispositivos IoT, y con EP en el desarrollo de un SDK quantum safe para aplicaciones móviles.

eurecat
Centre Tecnològic de Catalunya

COMPARACIÓN DE IMPLEMENTACIONES

Simulando una red real

- Eligiendo HW reducido en recursos compatible con SmartMeters
- Valorando distintos lenguajes/librerías para su uso en producción



ARDUINO

MicroPython

Embedded

Simulación y comparación por software

- Comparar distintos algoritmos post-cuanticos por su velocidad de ejecución

•Un nodo central - Dos concentradores - Cuatro smart meters, asociados dos a dos a los concentradores.

El nodo central ejecuta el intercambio de claves con cada concentrador, por tanto se generan 2 claves privadas. Las claves privadas de los concentradores son heredadas por los smart meters asociados. Las medidas se representan en milisegundos

Kyber512 **Intercambio de claves: 0.616** **smart meter: 21.441** **concentrador: 0.001** **nodo central: 66.405** **total simulación: 143.754**	**Kyber512-90s** **Intercambio de claves: 1.056** **smart meter: 25.128** **concentrador: 0.001** **nodo central: 63.988** **total simulación: 151.694**
LightSaber-KEM Intercambio de claves: 0.934 smart meter: 26.159 concentrador: 0.001 nodo central: 69.888 total simulación: 163.785	NewHope-512-CCA Intercambio de claves: 3.199 smart meter: 42.489 concentrador: 0.001 nodo central: 63.545 total simulación: 164.873
NTRU-HPS-2048-509 Intercambio de claves: 24.921 smart meter: 23.181 concentrador: 0.001 nodo central: 67.404 total simulación: 178.138	NTRU-HPS-2048-677 Intercambio de claves: 38.856 smart meter: 18.941 concentrador: 0.001 nodo central: 66.989 total simulación: 182.362

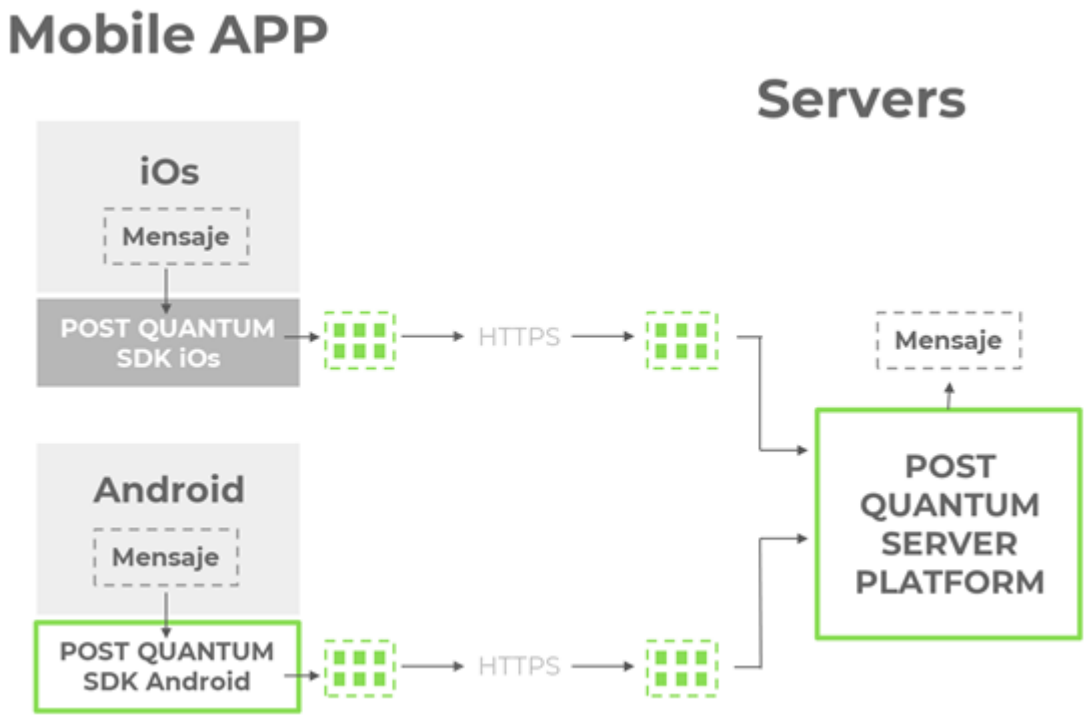
NTRU-HPS-4096-821 **Intercambio de claves: 88.219** **smart meter: 19.14** **concentrador: 0.001** **nodo central: 64.924** **total simulación: 229.18**	**NTRU-HRSS-701** **Intercambio de claves: 40.703** **smart meter: 18.701** **concentrador: 0.001** **nodo central: 67.916** **total simulación: 185.158**
SIKE-p434 intercanvi de claus: 68.518 smart meter: 19.767 concentrador: 0.001 nodo central: 67.061 total simulación: 314.013	SIKE-p434-compressed intercanvi de claus: 248.003 smart meter: 18.376 concentrador: 0.001 nodo central: 66.569 total simulación: 387.603
SIKE-p503 intercanvi de claus: 281.074 smart meter: 17.779 concentrador: 0.001 nodo central: 61.576 total simulación: 412.165	

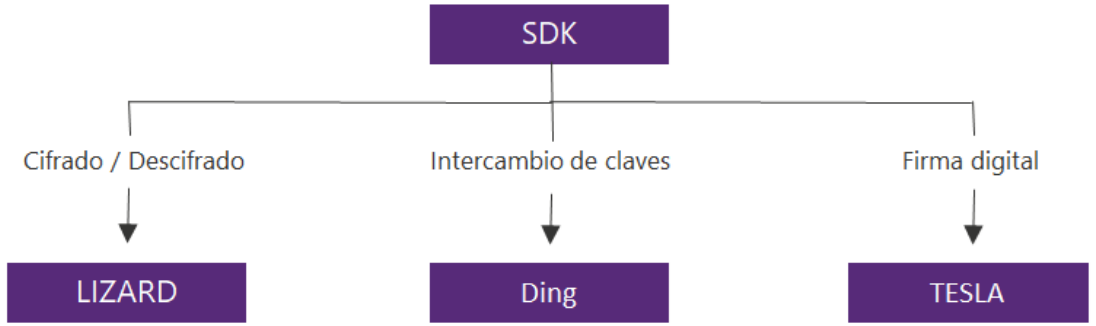
ACCIÓ Generalitat de Catalunya
Unió Europea
Fons Europeu
de Desenvolupament Regional

ACCIÓ Generalitat de Catalunya
Unió Europea
Fons Europeu
de Desenvolupament Regional

eurecat
Centre Tecnològic de Catalunya

Post Quantum SDK





Entanglement Partners_ >

eurecat
Centre Tecnològic de Catalunya

CONCLUSIONES

- La experiencia nos dice que **las migraciones y adopciones criptográficas llevan su tiempo**.
- La transición hacia la criptografía postcuántica es un **movimiento sin precedentes**.
- Los **estándares son más que necesarios** pero no se han de precipitar los acontecimientos.
- Los **retículos** parecen ser la apuesta más segura pero aún es pronto para asegurarlo.
- Con el diseño de los algoritmos no se acaba el proceso, **su implementación también es clave**.

eurecat
Centre Tecnològic de Catalunya

Gracias

Dr. Juan Caubet
juan.caubet@eurecat.org
@juancaubet

Director de la Unidad de IT&OT Security