

XI
JORNADAS
STIC
CCN-CERT

Ciberamenazas_
El reto de compartir

#XIJornadasCCNCERT

MADRID.
13 Y 14 DE DICIEMBRE
2017

Frente al computador cuántico, Criptografía postcuántica



- **Luis Hernández Encinas**[⊕]
- **Víctor Gayoso Martínez**[⊕]
- **David Arroyo Guardeno**[⊗]



- [⊕] Instituto de Tecnologías Físicas y de la Información (ITEFI)
Consejo Superior de Investigaciones Científicas (CSIC)
- [⊗] Escuela Politécnica Superior
Universidad Autónoma de Madrid (UAM)



[⊕] {luis, victor.gayoso}@iec.csic.es

[⊗] david.arroyo@uam.es

Índice

- 1. Introducción**
- 2. Criptografía cuántica**
- 3. Criptografía postcuántica**
 - 3.1. Criptografía basada en Teoría de Códigos**
 - 3.2. Firmas digitales basadas en hashes**
 - 3.3. Criptografía multivariante cuadrática**
 - 3.4. Criptografía basada en isogenias de curvas elípticas supersingulares**
 - 3.5. Criptografía basada en retículos**
- 4. Conclusiones**

1. Introducción

¿Ha muerto la criptografía que usamos hoy?



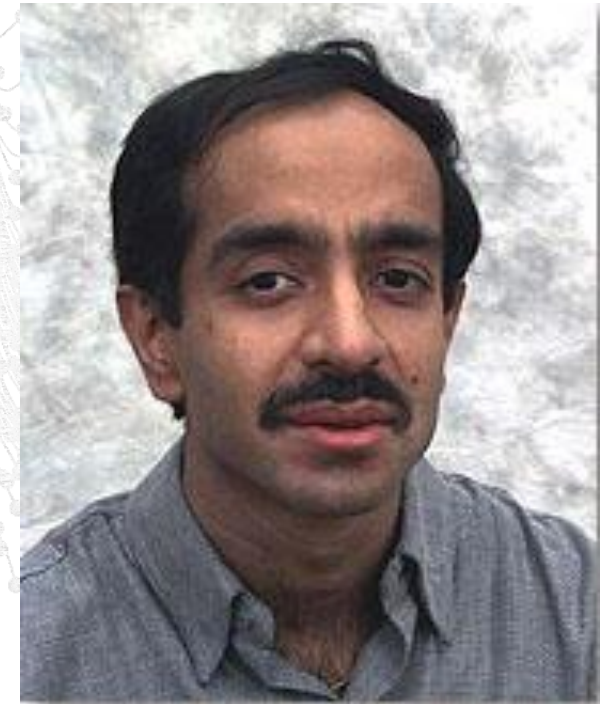
En 1997 (1994/95), Peter W. Shor publicó un artículo titulado “***Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer***”

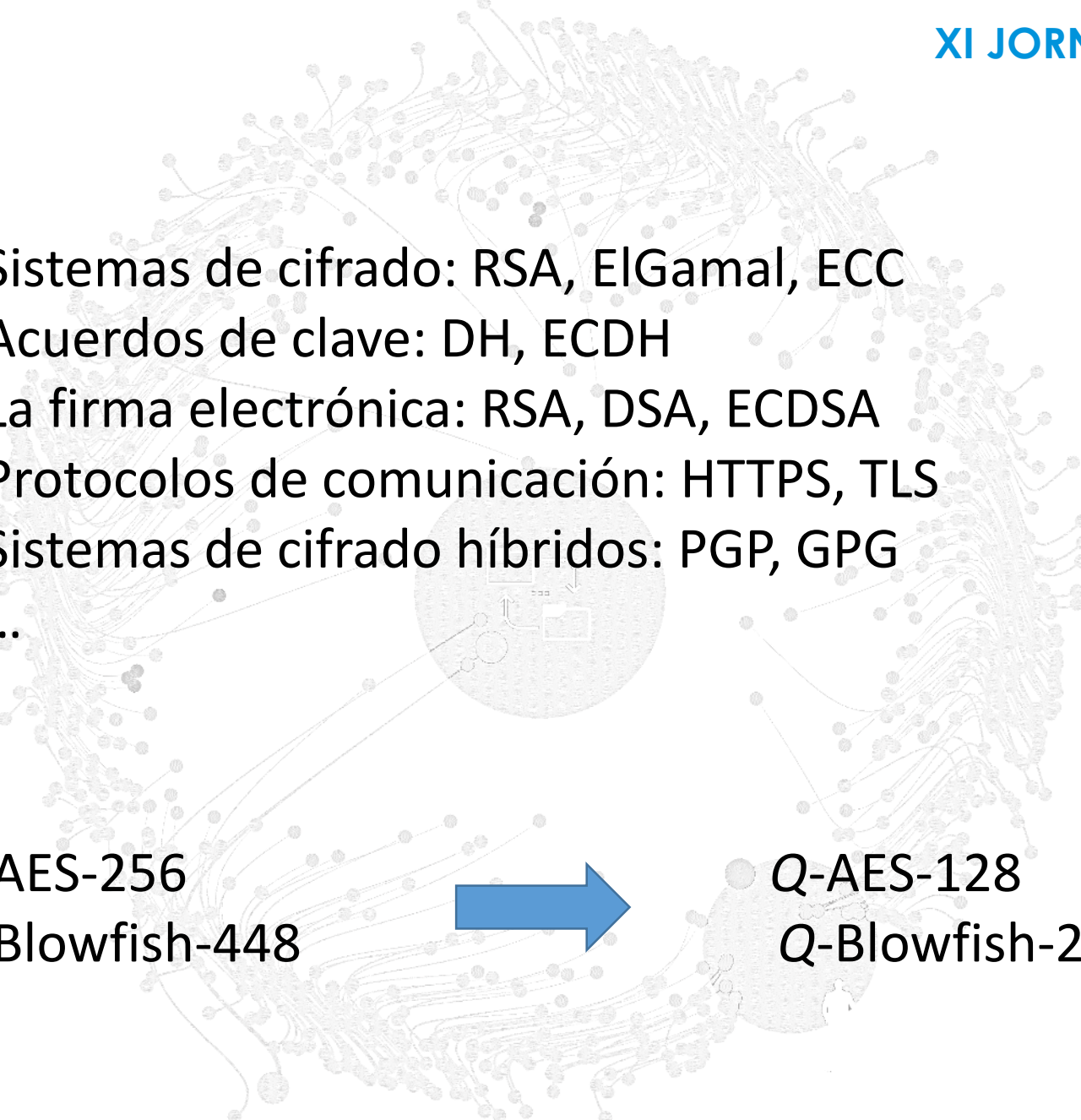
Estos algoritmos puede **romper en tiempo polinómico** algunos problemas matemáticos de la teoría de números utilizados en la **criptografía asimétrica** moderna, si existiera un ordenador cuántico

También en 1997, K.L. Grover publicó el artículo
***“Quantum mechanics helps in searching for a needle
in a haystack”***

Con este algoritmo, la computación cuántica reduciría
el tiempo necesario para romper la **criptografía
simétrica** a la **raíz cuadrada** del tiempo actual

Un ordenador cuántico tardaría el mismo tiempo en
realizar una búsqueda exhaustiva en un espacio de
claves de 256 bits (2^{256} claves) que un ordenador
actual en un espacio de claves de 128 bits (2^{128} claves)



- 
- ☹️ Sistemas de cifrado: RSA, ElGamal, ECC
 - ☹️ Acuerdos de clave: DH, ECDH
 - ☹️ La firma electrónica: RSA, DSA, ECDSA
 - ☹️ Protocolos de comunicación: HTTPS, TLS
 - ☹️ Sistemas de cifrado híbridos: PGP, GPG
 - ☹️ ...

😊 AES-256

😊 Blowfish-448



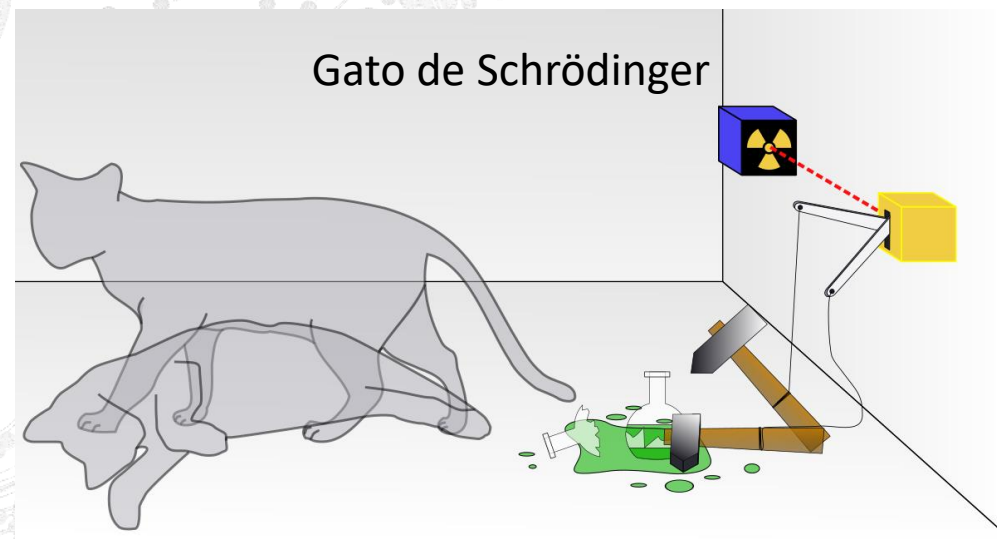
Q-AES-128

Q-Blowfish-224

2. Criptografía cuántica

La información en la **mecánica cuántica** se representa mediante valores discretos, como la transmisión de fotones polarizados (fibra óptica o espacio libre)

Todo **cuanto** (cantidad mínima de materia, energía, etc.) está a la vez en varios estados superpuestos hasta que es medido (temperatura, polarización, etc.), momento en el que se fija su estado (*Teorema de imposibilidad de clonación*)

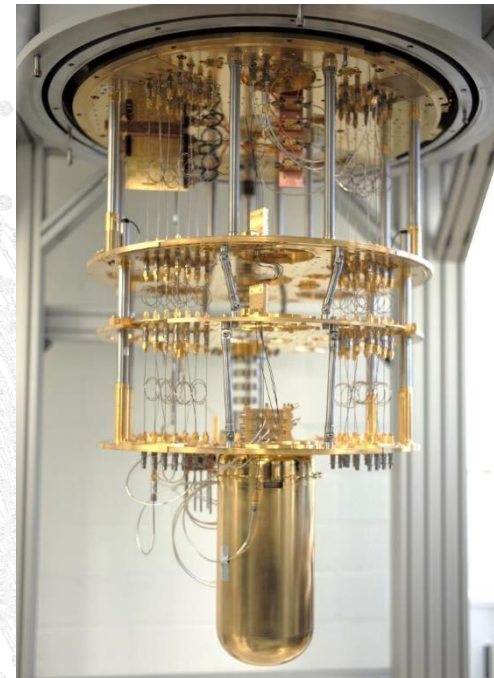


Información y protocolos de la criptografía cuántica

- La unidad mínima de información cuántica se denomina **qubit** (*quantum bit, qb*) y puede estar en los dos estados tradicionales y en ambos a la vez: $|0\rangle$, $|1\rangle$, $|0\rangle$ y $|1\rangle$
- La potencia de cálculo de un ordenador cuántico podría llegar a la de **100 millones** de ordenadores actuales
- Los únicos protocolos cuánticos propuestos son los de **distribución cuántica de claves** (por ejemplo, Bennett y Brassard-1984 y Ekert-1991) y se basan en el envío y medición de fotones polarizados

¿Llegará algún día el PC cuántico?

- **IBM Q** quiere construir antes de 10 años un ordenador cuántico (universal) de 50 *qb*. El actual tiene 16 *qb*
- **Google** afirma tenerlo todo listo para construir un ordenador cuántico de 49 *qb*
- **Microsoft** pretende construir un ordenador cuántico (topológico) capaz de ejecutar aplicaciones reales



Criostato (-270º C.) del ordenador cuántico universal de IBM Q

Sin embargo, romper los problemas matemáticos para las claves actuales (unos 2.000 bits) requeriría **4 días** con un ordenador cuántico de unos **7 millones de qb**

**Cuando aparezca un ordenador cuántico
con la potencia de cómputo adecuada...**



- Morirá la criptografía asimétrica basada en
 - **La factorización de números enteros**
 - **El cálculo de logaritmos discretos**
- La criptografía simétrica, solo necesitará **duplicar el tamaño de las claves** usadas hoy para sobrevivir, manteniendo la misma seguridad

3. Criptografía postcuántica (PQC)

(Bernstein *et al.*-2009)

La esperanza para la criptografía asimétrica está en estudiar **nuevos y viejos problemas matemáticos** para los que no haya algoritmos conocidos que los rompan o que no sean vulnerables a la computación cuántica, cuando llegue

- ✓ **Criptografía basada en Teoría de Códigos (Code-based)**
- ✓ **Firmas digitales basadas en hashes (Hash-based)**
- ✓ **Criptografía multivariante cuadrática (MQC)**
- ✓ **Criptografía basada en isogenias (Isogeny-based)**
- ✓ **Criptografía basada en retículos (Lattice-based)**

3.1 Criptografía basada en Teoría de Códigos (Code-based)

(McEliece-1978)

- La **clave pública** es una matriz M (**código de Goppa oculto**) de tamaño $dt \times n$ en $\mathbf{F}_2$, $n = 4b$, $d = \lceil \lg n \rceil$, $t = \lfloor n/2d \rfloor$
[1788 x 3582 elementos en $\mathbf{F}_2$]
- El **texto claro**, m , es una cadena de n bits con peso t
[3582 bits, 149 unos]
- El **texto cifrado** es un producto de matrices, $M \cdot m$, con dt bits
[1788 bits]
- El atacante debe deshacer la multiplicación por M
- No se conocen ataques para detectar estos códigos de Goppa

[nivel de seguridad de $b = 2^7 = 128$ bits, $n = 3582$, $d = 12$, $t = 149$]

3.2 Firmas digitales basadas en hashes (Hash-based)

(Merkle-1979)

Para firmar un mensaje se genera una cadena aleatoria y se calcula un hash como función de la cadena y del mensaje a firmar (**árboles de Merkle**)

- Hace falta una **función hash** de $2b$ bits [256 bits]
- La **clave pública** del firmante son $4b$ cadenas de $2b$ bits: $8b^2$ bits [16 kb]
- La **firma de un mensaje** tiene $2b+1$ cadenas de $2b$ bits: $2b(b+1)$ bits [8 kb]

[nivel de seguridad de $b = 128$ bits]

3.3 Criptografía Multivariante Cuadrática (MQC)

(Patarin-1996)

Una propuesta de la MQC se basa en la dificultad de **resolver un sistema cuadrático de ecuaciones mutivariantes en un cuerpo finito** (problema del isomorfismo de polinomios)

- La **clave pública** es una secuencia de $2b$ polinomios, de grado a lo sumo 2, en $4b$ variables y con coeficientes en $\mathbf{F}_2$: $16b^3+4b^2+2b$ bits
[4 Mb]
- La **firma** de un mensaje tiene $6b$ bits (corta)
[768 bits]
- La **verificación** de una firma requiere b^3 operaciones bit

[nivel de seguridad de $b = 128$ bits]

3.4 Criptografía basada en isogenias de curvas elípticas supersingulares

(Couveignes, 2006)

Isogenia: aplicación racional, $\phi: E \rightarrow E'$, entre dos curvas elípticas que preserva la estructura de grupo asociada (homomorfismo de grupos)

Supersingulares: las curvas no singulares han sido rotas

- Protocolos de **acuerdo de clave** tipo DH
- **Cifrado, firma y hashes**
- No se conocen algoritmos que puedan romper el problema base

3.5 Criptografía basada en Retículos (Lattice-based)

(Atjai-1996)

Se basa en el problema del **Aprendizaje con Errores** (LWE, aprendizaje automático o *machine learning*) y en una versión definida sobre un anillo: **Ring-LWE**

- Protocolos de **acuerdo de clave** tipo DH (basados en distribuciones estadísticas y R-LWE): Peikert-2014, Bos *et al.*-2015 y Alkim *et al.*-2015 (NewHope)
- **Cifrado, firma y hashes**: NTRU, Ajtai-Dwork (basados en LWE)
- No se conocen algoritmos que puedan vulnerar estos protocolos

4. Conclusiones

Protocolos/Algoritmos Criptográficos seguros con $\approx 2^b$ operaciones

Criptografía precuántica

- 3DES: $b = 128$ bits
- AES: $128 \leq b \leq 256$ bits
- RSA: módulo de $b^{3+o(1)}$ -bit
- McElice: longitud de código $b^{1+o(1)}$
- Merkle (firma) con hash de $b^{1+o(1)}$ bits
- Buchmann-Williams con discriminante de $b^{1+o(1)}$ bits
- ECDSA con curva de $b^{1+o(1)}$ bits
- HFE^v: con $b^{1+o(1)}$ polinomios
- NTRU (cifrado y firma): con $b^{1+o(1)}$ bits
- BCNS, NewHope (acuerdo de clave)

Criptografía postcuántica

-
- AES: $b = 128$ -bit
-
- McElice: longitud de código $b^{1+o(1)}$
- Merkle firma con hash de $b^{1+o(1)}$ bits
-
-
- HFE^v: con $b^{1+o(1)}$ polinomios
- NTRU (cifrado y firma): con $b^{1+o(1)}$ bits
- BCNS, NewHope (acuerdo de clave)

Futuro de la criptografía asimétrica

- Lattice challenge de la TU Darmstadt
- Call for Proposals del NIST

No estamos preparados para la PQC
Necesitamos más tiempo para

- Mejorar su eficiencia
- Conseguir confianza
- Mejorar su usabilidad

TU DARMSTADT
LATTICE
CHALLENGE

Call for Proposals

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce



▶ NIST is calling for quantum-resistant cryptographic algorithms for new public-key crypto standards

- Digital signatures
- Encryption/key-establishment

▶ We see our role as managing a process of achieving community consensus in a transparent and timely manner

▶ We do not expect to "pick a winner"

- Ideally, several algorithms will emerge as 'good choices'

▶ We may pick one (or more) for standardization

- Only algorithms publicly submitted considered

- ▶ Fall 2016 – formal Call For Proposals
- ▶ Nov 2017 – Deadline for submissions
- ▶ 3–5 years – Analysis phase
 - NIST will report its findings
- ▶ 2 years later – Draft standards ready

Referencias

- M. Ajtai, Generating Hard Instances of Lattice Problem, *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing* 99-108, 1996
- E. Alkim, L. Ducas, T. Pöppelmann, and P. Schwabe, Post-quantum key exchange - a new hope, *Cryptology ePrint Archive*, Report 2015/1092
- C.H. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, *IEEE International Conference on Computers, Systems and Signal Processing*, 8, 1984
- D.J. Bernstein, J. Buchmann, and E. Dahmen (Eds.), Post-Quantum Cryptography, Springer, Heidelberg, 2009
- J. W. Bos, C. Costello, M. Naehrig, and D. Stebila, Post-quantum key exchange for the TLS protocol from the ring learning with errors problem, *IEEE Symposium on Security and Privacy*, 553-570, 2015
- J.M. Couveignes. Hard homogeneous spaces, *IACR Cryptology ePrint Archive*, 2006/291
- A.K. Ekert, Quantum cryptography based on Bell's theorem, *Phys. Rev. Lett.* 67 (1991), 661-663
- K.L. Grover, Quantum mechanics helps in searching for a needle in a haystack, *Phys. Rev. Lett.* 79 (1997), 325-328
- R.C. Merkle, A certified digital signature, *Lecture Notes Comput. Sci.* 435 (1989), 218-238
- R.J. McEliece, A public-key cryptosystem based on algebraic coding theory, *DSN Progress Report* 44 (1978), 114-116
- NTRU, Quantum-Resistant High Performance Cryptography, <https://tbuktu.github.io/ntru/>
- J. Patarin, Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP): Two New Families of Asymmetric Algorithms, *Lecture Notes Comput. Sci.* 1070 (1996), 33-48
- C. Peikert, Lattice cryptography for the internet, *Lecture Notes Comput. Sci.* 8772 (2014), 197-219
- P.W. Shor, Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer, *SIAM J. Computing* 5, 26 (1997), 1484-1509

➤ E-Mails

- info@ccn-cert.cni.es
- ccn@cni.es
- sat-inet@ccn-cert.cni.es
- sat-sara@ccn-cert.cni.es
- organismo.certificacion@cni.es

➤ Websites

- www.ccn.cni.es
- www.ccn-cert.cni.es
- www.oc.ccn.cni.es

➤ Síguenos en

