



Criptografía Post Cuántica

[PARA MUGGLES]

María Isabel González Vasco

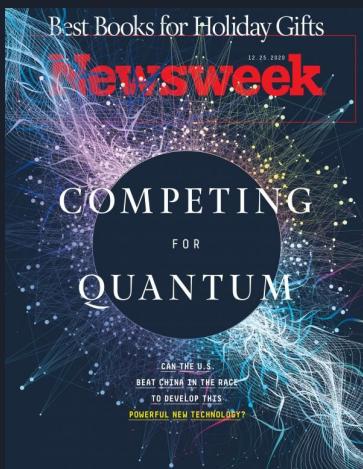
Universidad Carlos III de Madrid
[@maribelcrypt_vasco](https://twitter.com/maribelcrypt_vasco)

Cripto post—¿qué?

Desde los años 80, la computación cuántica se presenta como un elemento de cambio en los principios básicos de la

COMPLEJIDAD COMPUTACIONAL

que sustentan la criptografía moderna



A screenshot of a news article from WSJ Opinion. The title is 'The Quantum Computing Threat to American Security'. The subtitle reads: 'Google claims supremacy, but the risk remains that U.S. complacency lets China crack all its codes.' The author is Arthur Herman, and the date is Nov 10, 2019, 1:45 pm ET. There are share buttons for Facebook, Twitter, LinkedIn, and Print. A small image of a quantum computer chip is shown at the bottom.



A screenshot of an article from Scientific American. The title is 'Google's Quantum Computer Achieves Chemistry Milestone'. Below the title, it says 'A downsized version of the company's Sycamore chip performed a record-breaking simulation of a chemical reaction'. The author is Neil Savage, and the date is September 4, 2020. The article is categorized under 'QUANTUM COMPUTING'. At the bottom, there are links for COVID, Health, Mind & Brain, Environment, Technology, Space & Physics, Video, Podcasts, Opinion, Store, and a 'Sign in | Newsletter' button. There is also a 'Support science journalism.' link and a 'See My Options' button.



“He saw the hands that build...can also pull down” U2 [Exit]

TECNOLOGÍA CUÁNTICA QUE CONSTRUYE

Los protocolos QKD de distribución cuántica de claves permiten construir y transmitir claves criptográficas seguras con *muy buenas* propiedades de seguridad



“He saw the hands that build...can also pull down” U2 [Exit]

TECNOLOGÍA CUÁNTICA QUE CONSTRUYE

Los protocolos QKD de distribución cuántica de claves permiten construir y transmitir claves criptográficas seguras con *muy buenas* propiedades de seguridad

TECNOLOGÍA CUÁNTICA QUE DESTRUYE

Los algoritmos cuánticos para criptanálisis son capaces de vulnerar la seguridad de esquemas de cifrado y firma ampliamente utilizados e implementados



La amenaza cuántica: vectores reales de ataque

ALGORITMO DE GROVER

Permite la búsqueda de un elemento en una lista no estructurada

USO: Búsqueda/testeo de claves criptográficas utilizadas en herramientas simétricas

VÍCTIMAS: MACs, Cifradores de Bloque, Funciones Hash, etc. (AES, SHA, HMAC...)

CONTRAMEDIDA: claves de mayor longitud (2x)



La amenaza cuántica: vectores reales de ataque

ALGORITMO DE GROVER

Permite la búsqueda de un elemento en una lista no estructurada

USO: Búsqueda/testeo de claves criptográficas utilizadas en herramientas simétricas

VÍCTIMAS: MACs, Cifradores de Bloque, Funciones Hash, etc. (AES, SHA, HMAC...)

CONTRAMEDIDA: claves de mayor longitud (2x)

ALGORITMO DE SHOR

Dada una función periódica que podemos evaluar en modo “caja negra”, permite calcular su periodo

USO: Resolución eficiente del problema de factorización de enteros y el problema del logaritmo discreto

VÍCTIMAS: Algoritmos de cifrado/firma tipo RSA o Diffie-Hellman (RSA-OAEP, DSA, ECDSA, etc.)

CONTRAMEDIDA: migración a otro tipo de criptografía de clave pública ... CRIPTOGRAFÍA POST-CUÁNTICA

Piezas para el puzzle Post-cuántico





Algunas pinceladas

HASHES

Como herramienta simétrica, se adaptan aumentando rangos
(tamaños de conjuntos de búsqueda)



Algunas pinceladas

HASHES

RETÍCULOS Y CÓDIGOS

Como herramienta simétrica, se adaptan aumentando rangos
(tamaños de conjuntos de búsqueda)

Involucran problemas de “decodificación con ruido” para los
que no se conocen algoritmos cuánticos eficientes



Algunas pinceladas

HASHES

Como herramienta simétrica, se adaptan aumentando rangos
(tamaños de conjuntos de búsqueda)

RETÍCULOS Y CÓDIGOS

Involucran problemas de “decodificación con ruido” para los
que no se conocen algoritmos cuánticos eficientes

ISOGENIAS

Construcciones algebraico-geométricas... (mejor lo
hablamos otro día...el verano ha sido duro..)

Algunas pinceladas

HASHES

RETÍCULOS Y CÓDIGOS

ISOGENIAS

OTROS

Como herramienta simétrica, se adaptan aumentando rangos
(tamaños de conjuntos de búsqueda)

Involucran problemas de “decodificación con ruido” para los que no se conocen algoritmos cuánticos eficientes

Construcciones algebraico-geométricas... (mejor lo hablamos otro día...el verano ha sido duro..)

¡SIGUE BUSCANDO!





Primeros estándares (Julio 2022)

CONSTRUCCIONES PARA KEY ENCAPSULATION (KEM)

CRYSTALS-Kyber

AVANZAN A RONDA 4 (+2 AÑOS)

- ClassicMcEliece
- BIKE
- HQC
- SIKE



Primeros estándares (Julio 2022)



CONSTRUCCIONES PARA KEY ENCAPSULATION (KEM)

CRYSTALS-Kyber

AVANZAN A RONDA 4 (+2 AÑOS)

- ClassicMcEliece
- BIKE
- HQC
- SIKE

CONSTRUCCIONES PARA FIRMA DIGITAL

- CRYSTALS-Dilithium
- FALCON
- SPHINCS+

¡¡NUEVA COMPETICIÓN EN MARCHA!!

Pues... ya estaría... ¿o no?



¿Sabemos de verdad cómo se comportan los
adversarios cuánticos?

Pues... ya estaría... ¿o no?



¿Sabemos de verdad cómo se comportan los adversarios cuánticos?

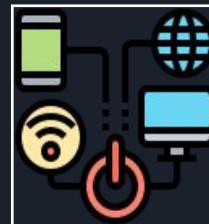


¿Es razonable una migración inmediata a sistemas post-cuánticos?

Pues... ya estaría... ¿o no?



¿Sabemos de verdad cómo se comportan los adversarios cuánticos?



¿Es razonable una migración inmediata a sistemas post-cuánticos?



Las construcciones post-cuánticas, ¿son seguras?

Últimas noticias...

Paper 2022/975
An efficient key recovery attack on SIDH

Wouter Castryck , KU Leuven
Thomas Decru , KU Leuven

Abstract

We present an efficient key recovery attack on the Supersingular Isogeny Diffie-Hellman protocol (SIDH). The attack is based on Kani's "reducibility criterion" for isogenies from products of elliptic curves and strongly relies on the torsion point images that Alice and Bob exchange during the protocol. If we assume knowledge of the endomorphism ring of the starting curve then the classical running time is polynomial in the input size (heuristically), apart from the factorization of a small number of integers that only depend on the system parameters. The attack is particularly fast and easy to implement if one of the parties uses 2-isogenies and the starting curve comes

Paper 2022/1452
A Side-Channel Attack on a Hardware Implementation of CRYSTALS-Kyber

Yanning Ji, KTH Royal Institute of Technology
Ruize Wang, KTH Royal Institute of Technology
Kalle Ngo, KTH Royal Institute of Technology
Elena Dubrova, KTH Royal Institute of Technology
Linus Backlund, KTH Royal Institute of Technology

Abstract

CRYSTALS-Kyber has been recently selected by the NIST as a new public-key encryption and key-establishment algorithm to be standardized. This makes it important to assess how well CRYSTALS-Kyber implementations withstand side-channel attacks. Software implementations of

Paper 2022/1410
Breaking and Protecting the Crystal: Side-Channel Analysis of Dilithium in Hardware

Hauke Steffen , TÜV Informationstechnik GmbH
Georg Land , Ruhr University Bochum, German Research Centre for Artificial Intelligence
Lucie Kogelheide , TÜV Informationstechnik GmbH
Tim Güneysu , Ruhr University Bochum, German Research Centre for Artificial Intelligence

Abstract

The lattice-based CRYSTALS-Dilithium signature schemes has been selected for standardization by the NIST. As part of the selection process, a large number of implementations for platforms like x86, ARM Cortex-M4, or - on the hardware side - Xilinx Artix-7 have been presented and discussed by experts. Moreover, the software implementations have been subject to side-

Metadata
Available format(s)
Category Attacks and cryptanalysis
Publication info Preprint.
Keywords FPGA, Side-Channel Analysis, SPA, CPA, PQC, Dilithium
Buscar -1°C 11



Últimas noticias...



Cryptology ePrint Archive

Paper 2022/975

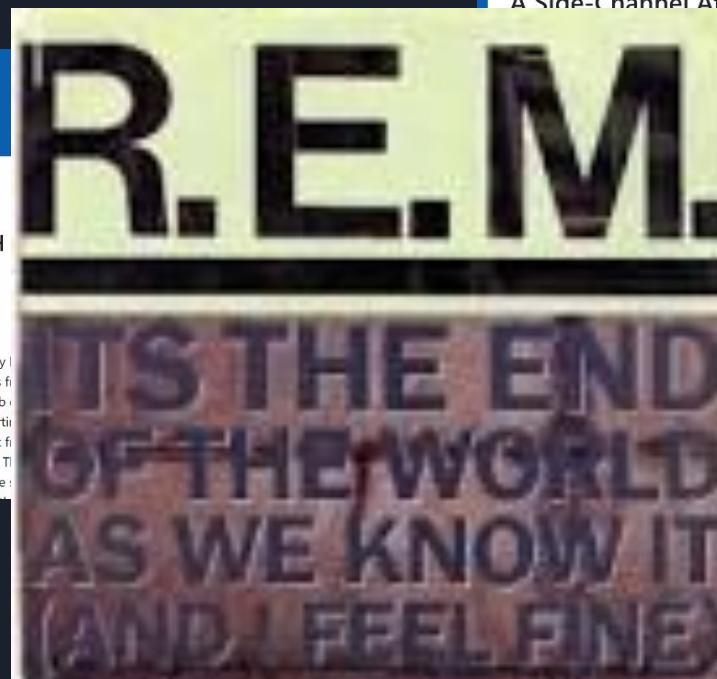
An efficient key recovery attack on SIDH

Wouter Castryck , KU Leuven

Thomas Decru , KU Leuven

Abstract

We present an efficient key recovery attack on the Supersingular Isogeny Diffie-Hellman (SIDH) protocol. The attack is based on Kani's "reducibility criterion" for isogenies from genus 2 curves and strongly relies on the torsion point images that Alice and Bob exchange during the protocol. If we assume knowledge of the endomorphism ring of the starting curve, the classical running time is polynomial in the input size (heuristically), apart from a small number of integers that only depend on the system parameters. The attack is fast and easy to implement if one of the parties uses 2-isogenies and the other party uses 3-isogenies.



The lattice-based CRYSTALS-Dilithium signature scheme has been selected for standardization by the NIST. As part of the selection process, a large number of implementations for platforms like x86, ARM Cortex-M4, or - on the hardware side - Xilinx Artix-7 have been presented and discussed by experts. Moreover, the software implementations have been subject to side-



Cryptology ePrint Archive

Paper 2022/1452

A Side-Channel Attack on a Hardware CRYSTALS-Kyber

Technology
Technology
chnology
of Technology
of Technology

selected by the NIST as a new public-key encryption and key-exchange standard. This makes it important to assess how well CRYSTALS-Kyber withstand side-channel attacks. Software implementations of

Papers ▾ Submissions ▾ About ▾

Metadata

Available format(s)



Category

Attacks and cryptanalysis

Publication info

Preprint

Keywords

FPGA

Side-Channel Analysis

SPA

CPA

PQC

Dilithium



Conclusión: Hacia una migración sensata

- Conócete a ti mismo (identifica dónde usas criptografía pre-cuántica y cuándo su seguridad es crítica). Valora el uso de soluciones híbridas.



Conclusión: Hacia una migración sensata

- Conócete a ti mismo (**identifica dónde usas criptografía pre-cuántica y cuándo su seguridad es crítica**). Valora el uso de soluciones **híbridas**.
- Sé modular. Todo ha de ser sustituible. (la llamada **cripto-agilidad** ha llegado para quedarse)



Conclusión: Hacia una migración sensata

- Conócete a ti mismo (**identifica dónde usas criptografía pre-cuántica y cuándo su seguridad es crítica**). Valora el uso de soluciones **híbridas**.
- Sé modular. Todo ha de ser sustituible (**la llamada cripto-agilidad ha llegado para quedarse**)
- Espera sorpresas en el camino (no pienses que el “largo plazo” será muy largo..)

Conclusión: Hacia una migración sensata

- Conócete a ti mismo (**identifica dónde usas criptografía pre-cuántica y cuándo su seguridad es crítica**). Valora el uso de soluciones **híbridas**.
- Sé modular. Todo ha de ser sustituible. (la llamada **cripto-agilidad** ha llegado para quedarse)
- Espera sorpresas en el camino (no pienses que el “largo plazo” será muy largo..)
- Estáte alerta... (sigue los avances y ataques que se publican....pero ¡mantén la calma!)





¡Gracias!

¿Preguntas?..... ¡Yo tengo muchas!

