ARSAT

CRYPTOCOMM:
FUNDAMENTOS ALGEBRAICOS PQC

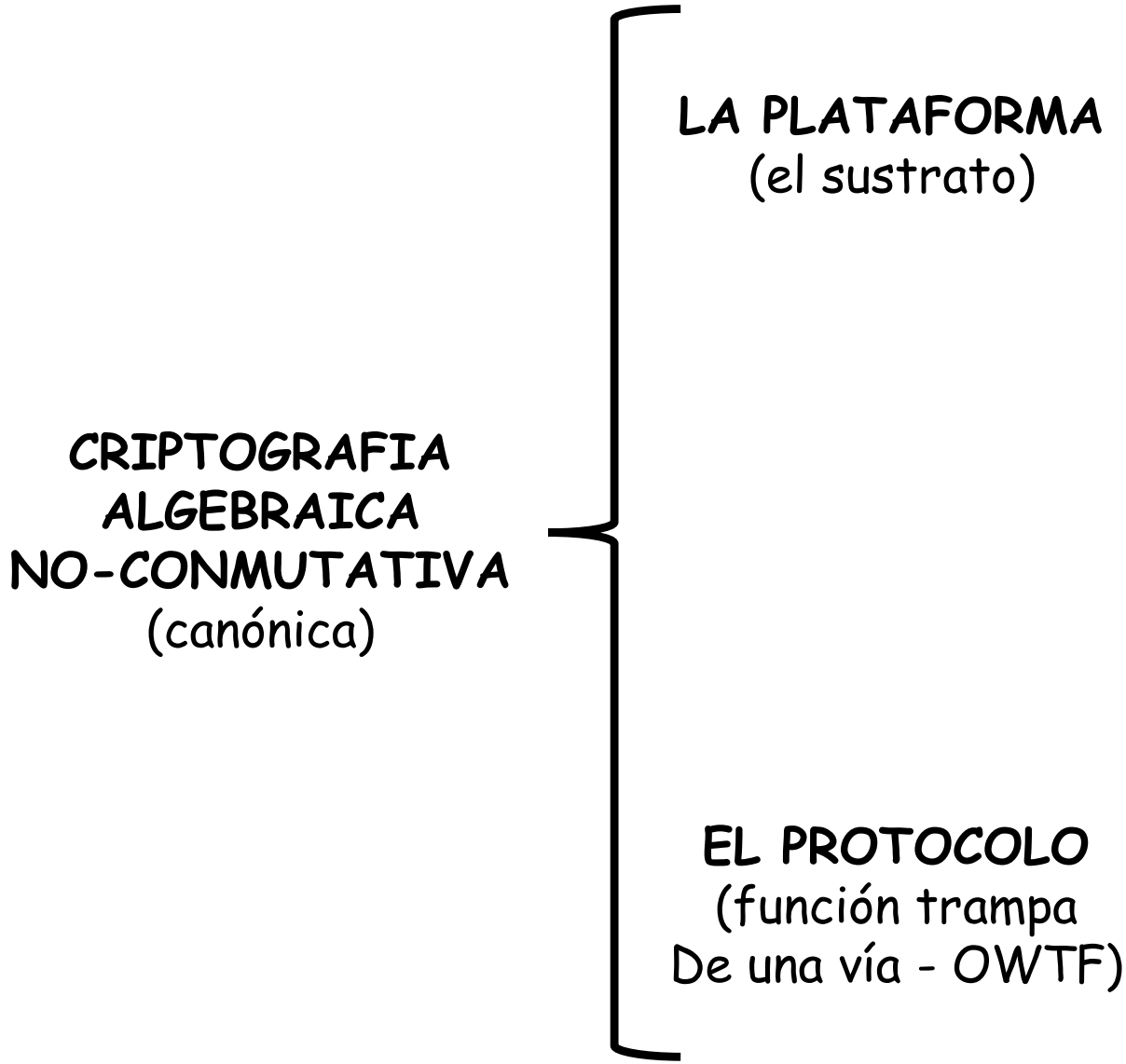
sistema de comunicaciones criptográficas postcuánticas

Dr Pedro Hecht – phecht@dc.uba.ar /qubit101@gmail.com

V.2.6.0

Frente a las soluciones tradicionales PQC consideradas por la compulsa NIST (USA) (consistentes en: códigos correctores lineales, retículos, sistemas multicuadráticos árboles de Merkle, isogenias elípticas, etc.) hemos desarrollado desde 2016 una línea original basada en protocolos canónicos extraídos de la Teoría Combinatoria de Grupos.

•"Post-Quantum Cryptography(PQC): Generalized ElGamal Cipher over GF(251^8)", Hecht P., ArXiv Cryptography and Security (cs.CR) http://arxiv.org/abs/1702.03587 6pp (2017) & Journal of Theoretical and Applied Informatics (TAAI), 28:4, pp 1-14 (2016), http://dx.doi.org/10.20904/284001
•"Post-Quantum Cryptography: A Zero-Knowledge Authentication Protocol", Hecht P., ArXiv Cryptography and Security (cs.CR) https://arxiv.org/abs/1703.08630, 3pp (2017)
•"Post-Quantum Cryptography: S381 Cyclic Subgroup of High Order", Hecht P., ArXiv Cryptography and Security (cs.CR) http://arxiv.org/abs/1704.07238 (preprint) & International Journal of Advanced Engineering Research and Science (IJAERS) 4:6, pp 78-86 (2017), https://dx.doi.org/10.22161/ijaers.4.6.10
•"PQC: Triple Decomposition Problem Applied To GL(d, Fp) - A Secure Framework For Canonical Non-Commutative Cryptography", Hecht P., ArXiv Cryptography and Security (cs.CR) https://arxiv.org/abs/1810.08983, 9pp (2018), DOI: 10.13140/RG.2.2.23240.78082
•"PQC: Extended Triple Decomposition Problem Applied To GL(d, Fp) – An Evolved Frmework For Canonical Non-Commutative Cryptography", Hecht P., ArXiv Cryptography and Security (cs.CR), https://arxiv.org/abs/1812.05454v1, 2pp (2018), DOI: 10.13140/RG.2.2.20242.09926
•"Algebraic Extension Ring Framework for Non-Commutative Asymmetric Cryptography ", Hecht P., ArXiv Cryptography and Security (cs.CR), https://arxiv.org/abs/2002.08343, 4pp (2020),
•"PQC: R-Propping of Public-Key Cryptosystems Using Polynomials over Non-commutative Algebraic Extension Rings", Hecht P., https://eprint.iacr.org/2020/1102, 10pp (2020) DOI: 10.13140/RG.2.2.25826.56002
•"R-Propping of HK17: Upgrade for a Detached Proposal of NIST PQC First Round Survey", Hecht P., https://eprint.iacr.org/2020/1217, 7pp (2020) DOI: 10.13140/RG.2.2.31287.96163
•"PQC: R-Propping of Burmester-Desmedt Conference Key Distribution System", Hecht P., https://eprint.iacr.org/2021/024, DOI:10.13140/RG.2.2.22638.43846 (2021)
•"PQC: R-Propping of a New Group-Based Digital Signature", Hecht P., https://eprint.iacr.org/2021/270 , DOI: 10.13140/RG.2.2.35795.91683 (2021)
•"PQC: R-Propping a Chaotic Cellular Automata", Hecht P., https://eprint.iacr.org/2021/672 , DOI: 10.13140/RG.2.2.11309.61924 (2021)
•"PQC: R-propping of a Simple Oblivious Transfer", Hecht P., https://eprint.iacr.org/2021/854, DOI: 10.13140/RG.2.2.13925.32489 (2021)


CRIPTOGRAFIA
ALGEBRAICA
NO-CONMUTATIVA
(canónica)
LA PLATAFORMA
(el sustrato)
EL PROTOCOLO
(función trampa
De una vía - OWTF)

LA PLATAFORMA

(el sustrato)

Se ha definido como plataforma un espacio de matrices cuadradas de bytes, de dimensionalidad paramétrica y en cuyas operaciones de álgebra lineal se reemplazan la suma modular (256) de bytes por el operador XOR (bit a bit) y el producto modular (256) como el producto de polinomios en el campo $GF(2^8)$.

El resultado es una estructura de anillo (Advanced Extension Ring: AER) cuya primer ley de composición forma un grupo conmutativo con identidad 0 (matriz nula) y cuya segunda ley de composición es un monoide no-conmutativo con identidad I (matriz identidad).

Esencialmente se han interpretado los bytes componentes de la matriz como polinomios booleanos de grado 7, que se suman y multiplican como tales, reduciéndolos modularmente con un polinomio primitivo de grado 8 (hay 30 disponibles). Por ese motivo, denominamos a las matrices AER como tensores de rango 3.

La enorme ventaja de este procedimiento es la pérdida de la linearidad interna, característica que bloquea los ataques de reducción lineal: *Algebraic Span* de Tsaban (2018) y los *Linearization Attacks* de Roman'kov (2017) y que son la base de la seguridad del AES (capas 1 y 3) (técnica que denominamos R-Propping, aplicable a cualquier protocolo pre-cuántico).

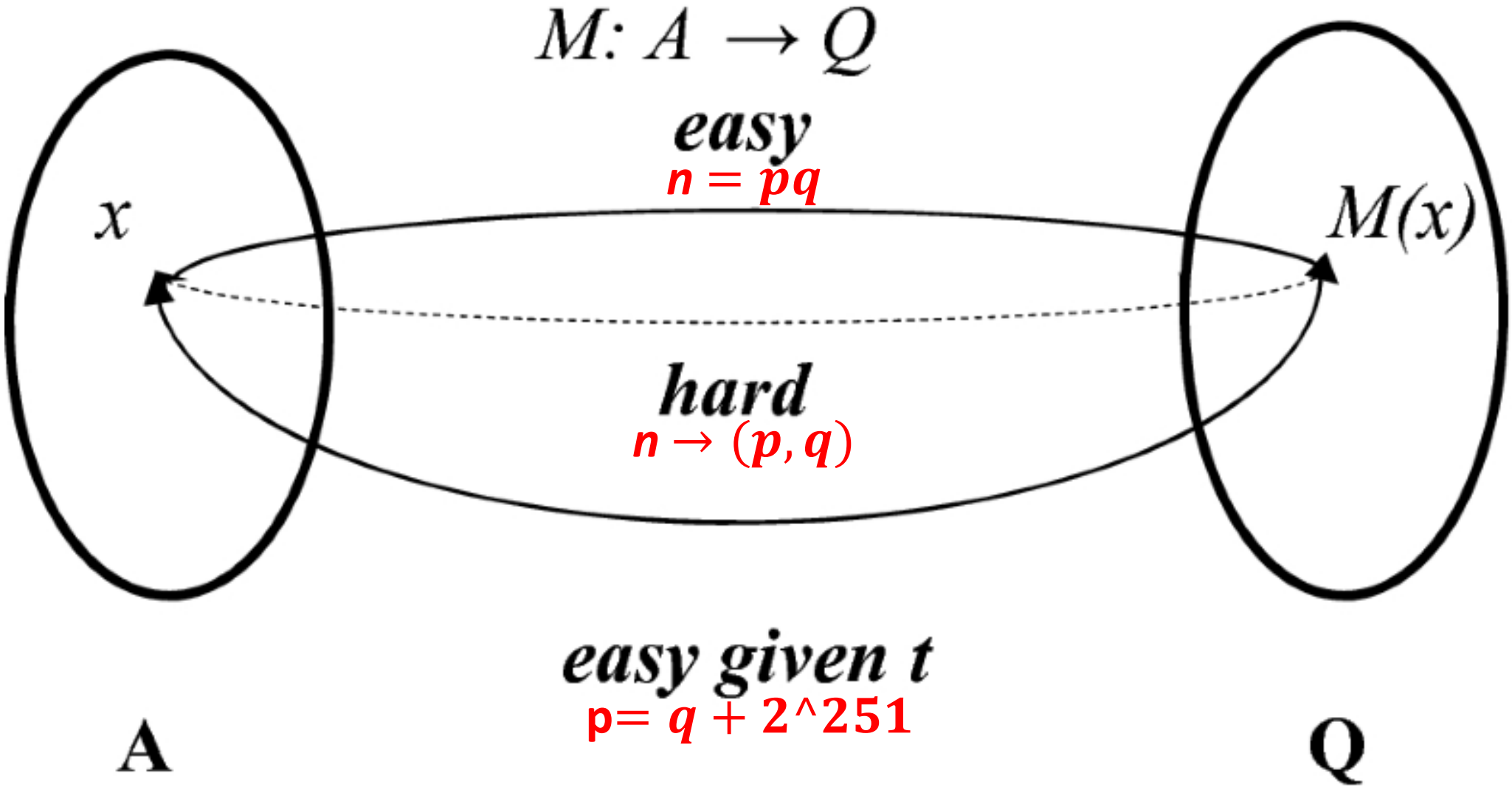
Finalmente, para fortalecer la plataforma, en vez de usar los tensores en forma directa, se usan las potencias de polinomios modulares (256) de tensores como unidades operativas.

$$f(A) = c_0.[A]^0 \oplus c_1.[A]^1 \oplus c_2.[A]^2 \oplus \ldots \oplus c_k.[A]^k$$

f(A) es la clave privada de cada entidad, el tensor A es público.

la potencia del polinomio $f^k(A)$ es la unidad operativa, Los coeficientes c_i son enteros (mod 256) en producto escalar y cada potencia matricial se define como $[A]^n=[A]\odot[A]\odot\ldots\odot[A]$ $(n\text{-veces})$, usando las operaciones de campo $GF(2^8)$

EL PROTOCOLO (función trampa de una vía - OWTF)


$M: A \rightarrow Q$
easy
$n = pq$
x
M(x)
hard
$n \rightarrow (p, q)$
easy given t
p= q + 2^251
A
Q

Los criptosistemas cuyos protocolos están basados en funciones trampa de una vía (OWTF), se definen como **canónicos**. En estructuras algebraicas no-conmutativas, las OWTF se derivan de los siguientes problemas que, por ahora, pertenecen a la clase de complejidad temporal NP. Aquí las unidades operativas son elementos de grupos algebraicos no-conmutativos.

Aquí se presentan algunos problemas base de las OWTF, en orden de complejidad creciente:

	dados	hallar	conociendo
CSP→ conjugator search problem	$y = z^{-1} x \ z$	$z \in G$	$(x, y) \in G \times G$
DCP→ double coset problem	$y = z_1 \ x \ z_2$	$z_1, z_2 \in G$	$(x, y) \in G \times G$
SDP→symmetric decomposition problem	$y = z^m x \ z^n$	$z \in G$	$(x, y) \in G \times G$ $m, n \in \mathbb{Z}$
GSDP→generalized symmetric decomposition problem	$y = z^m x \ z^n$	$z \in S$	$(x, y) \in G \times G$ y $S \subseteq G$ $m, n \in \mathbb{Z}$

Para su aplicación en el sistema CRYPTOCOMM, se ha optado por la OWTF basada en el problema GSDP por cumplir con seguridad semántica al nivel IND-CCA2, usando potencias de polinomios modulares como unidades operativas (z) y las indicadas operaciones de campo.

PARÁMETROS DE SEGURIDAD ***DATOS PÚBLICOS***

Dimensión de tensores [A],[B]: dim ≥ 16, cardinal 2^160

Grado del polinomio modular f(A): degree [20, 36]

Enteros (m, n): random[2, 2^{64}-2]

CLAVES PARA LA CRIPTOGRAFÍA ASIMÉTRICA

Obs: losTensores [A],[B] y los enteros (m,n) son datos públicos.

Polinomio modular f(A): ***CLAVE PRIVADA***

GSDP f(A)→ f^m(A) . [B] . f^n(A): ***CLAVE PÚBLICA***

CARACTERÍSTICAS y NORMAS DE SEGURIDAD QUE ALCANZA o SUPERA CRYPTOCOMM

PROTOCOLO ASIMÉTRICO

- Full PQC (NIST https://csrc.nist.gov/Projects/post-quantum-cryptography)
- R-Propping AER algebraic extensión ring structure (https://eprint.iacr.org/2020/1102)
- Hashing/HMAC Triple Sandwich/SHA3-512 (to be published)

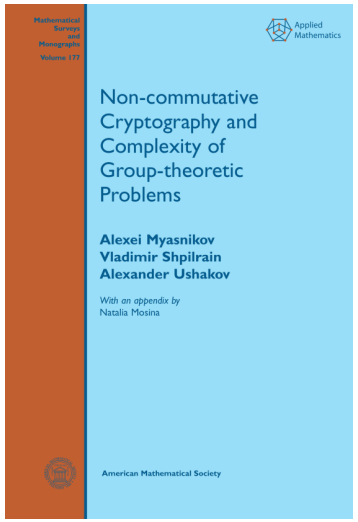
PLATAFORMA ASIMÉTRICA

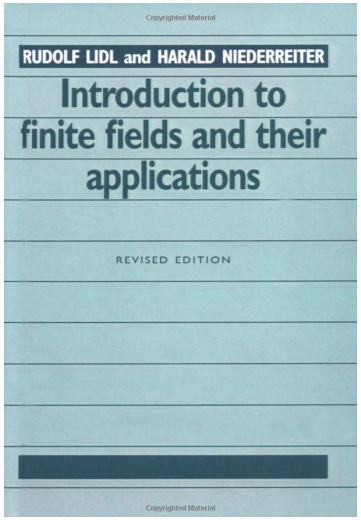
- ZT Architecture (NIST SP 800-207)
- IND-CCA2 semantic security compliance (https://courses.cs.ut.ee/2005/crypto-seminar-fall/slides/S5.Bogdanov.indcca2.pdf)
- NIST PQC CATEGORY 1 compliance (https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization/evaluation-criteria/security-(evaluation-criteria)
- Perfect backward & forward secrecy (https://avinetworks.com/glossary/perfect-forward-secrecy/)
- GSDP OWTF protection (https://eprint.iacr.org/2020/1102)
- PUBLIC KEY INFRASTRUCTURE AUTHENTICATION (https://www.keyfactor.com/resources/what-is-pki/)

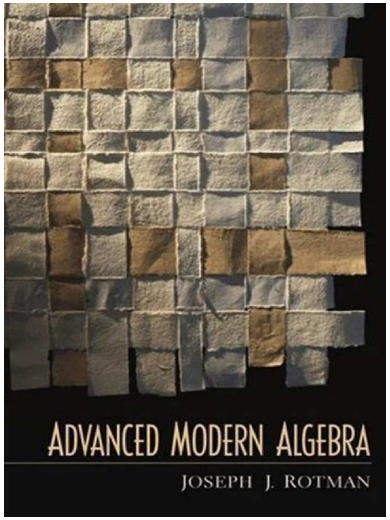
PLATAFORMA SIMÉTRICA (usada en modo híbrido)

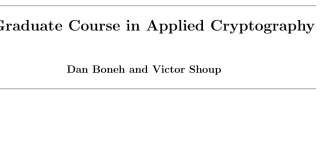
- AEAD-EtM/GCM (https://eprint.iacr.org/2009/215.pdf, http://toc.cryptobook.us/, https://csrc.nist.rip/groups/ST/toolkit/BCM/documents/proposedmodes/gcm/gcm-spec.pdf)

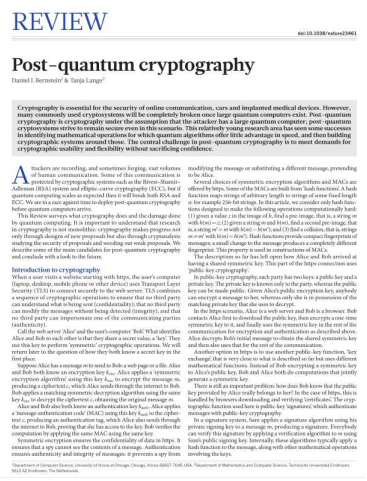
Bibliografía:

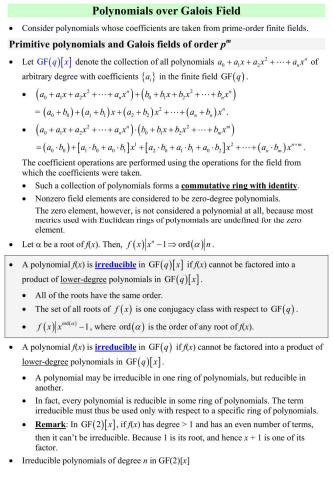












disponible por solicitud a qubit101@gmail.com