INTRODUCCIÓN A LA CRIPTOGRAFÍA POSTCUÁNTICA

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

A favor de la criptografía asimétrica convencional

- Amplia difusión
- Tres décadas de experiencia

En contra de la criptografía asimétrica convencional

- Empleo de bibliotecas de precisión extendida
- Alta dependencia de los motores generadores de seudoprimos
- Ataques de canal lateral por falla programada en hardware (NSA?) (Rabin, 1997)
- Ataques en motores CSPRBG (Dual_EC_DRBG -> NSA Snowden, 2013)
- Fuerte descrédito en la comunidad criptológica por recientes y significativos avances en la resolución del problema DLP (algoritmos *quasi-P* Barbulescu-Gaudry-Joux-Thomé, 2014)
- Ataques de complejidad subexponencial y algoritmos cuánticos (computadora cuántica NSA, 2015)

NETWORKWORLD News | Blogs | Newsletters | Videos | Events | Resources | INSIDER

Security | LANs & WANs | UC / VoIP | Cloud | Infrastructure Mgmt | Wireless | Software | Data Center

Anti-malware | Compliance | Cybercrime | Firewall & UTM | IDS/IPS | Endpoint Security | SIEM | White Pape

News

NSA backdoor fears creating crisis of confidence i U.S. high-tech products, services

Intel's CISO: We don't support any backdoors

By Ellen Messmer, Network World
October 09, 2013 01:39 PM ET

10 Comments Print

Network World - Fear convince U.S.-based for espionage purpos

There has been, of c documents leaked by neither the NSA nor th has frequently been th

New York Times provides NSA backdoor in crypto sp

The paper points a finger definitively at the long-suspec

by **Megan Geuss** - Sept 11 2013, 12:00am -0300

Today, the *New York Times* reported that an algorithm for generating random numbers, which was adopted in 2006 by the National Institute of Standards and

Cisco says controversial NIST crypto - potential NSA backdoor -- 'not invoked' in products

But Cisco engineer says "some of the libraries" in products can support Dual EC DRBG

By Ellen Messmer, Network World
October 17, 2013 03:48 PM ET

1 Comment Print Share 5 Like 0

Network World - Controversial crypto technology known as Dual EC DRBG, thoug be a backdoor for the National Security Agency, ended up in some Cisco products part of its code libraries. But Cisco says they cannot be used because it chose an crypto as an operational default which can't be changed.

Dual EC DRBG or Dual Elliptic Curve Deterministic Random Bit Generator (Dual E DRBG) from the National Institute of Standards and Technology and a crypto toolki from RSA is thought to have been one main way the crypto ended up in hundreds of vendors'

Slashdot Search this website ...

Business Intelligence Cloud DataCenter

RSA Security Warns of Possible NSA Backdoor

LONGFORM VIDEO REVIEWS TECH SCIENCE CULTURE DESIGN BUSINESS US & WOR

RSA tells developers to stop using encryption with suspected NSA backdoor

By Jeff Blagdon on September 20, 2013 03:33 pm Email @jblagdon

DON'T MISS STORIES FOLLOW THE VERGE Like 192k Follow 305K followers

Snowden's NSA post in Hawaii failed to install "anti-leak" software

New York Times provides new details about NSA backdoor in crypto spec

The paper points a finger definitively at the long-suspected Dual_EC_DRBG algorithm.

by **Megan Geuss** - Sept 11 2013, 12:00am -0300

HACKING PRIVACY 85

Today, the *New York Times* reported that an algorithm for generating random numbers, which was adopted in 2006 by the National Institute of Standards and Technology (NIST), contains a backdoor for the NSA. The news followed a *NYT* report from last week, which indicated that the National Security Agency (NSA) had

NSA LEAKS

Snowden's NSA post in Hawaii failed to install "anti-leak" software

National Security

NSA seeks to build quantum computer that could crack most types of encryption

The development of a quantum computer has long been a goal of many in the scientific community, with revolutionary implications for fields such as medicine as well as for the NSA's code-breaking mission. With such technology, all current forms of public key encryption would be broken, including those used on many secure Web sites as well as the type used to protect state secrets.

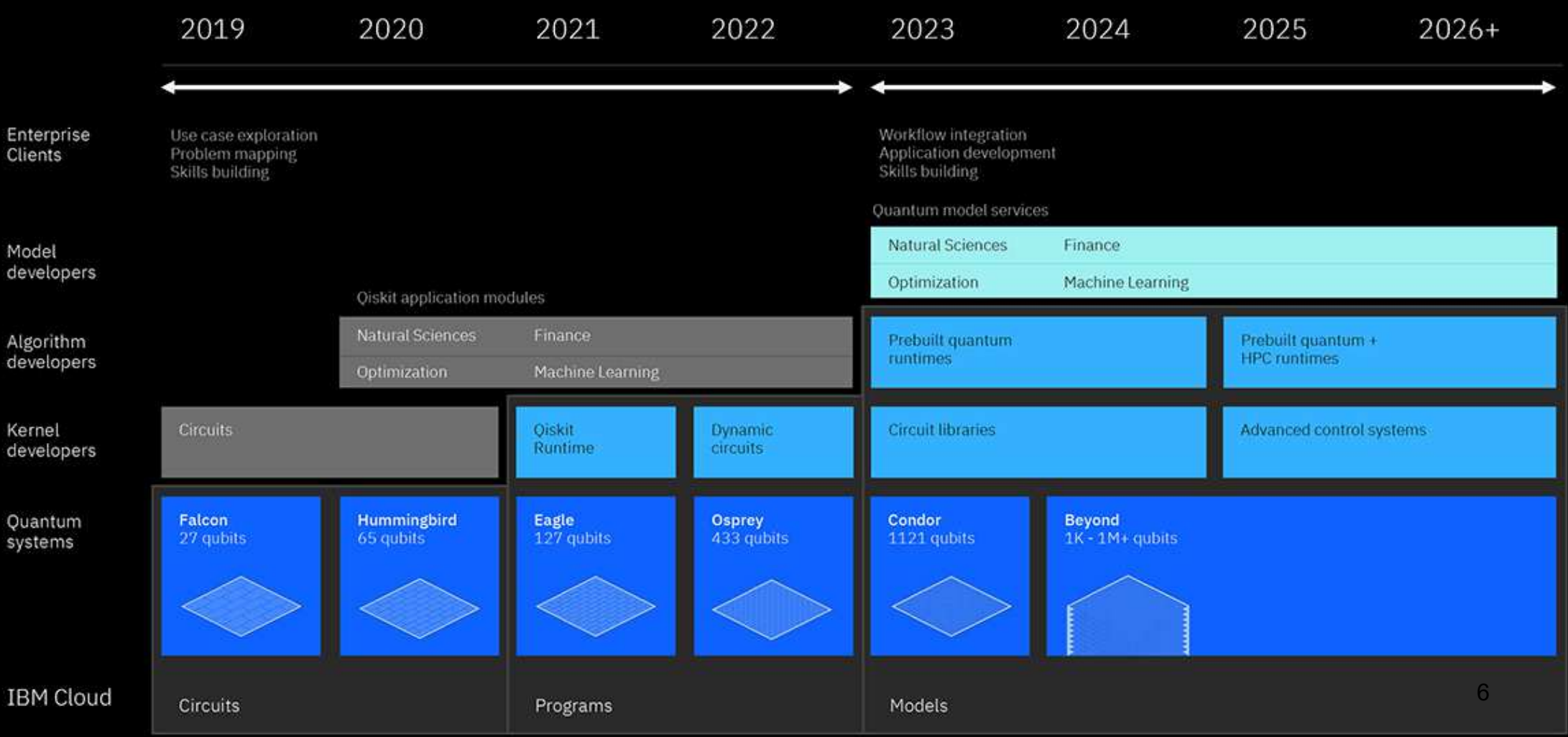
Physicists and computer scientists have long speculated about whether the NSA's efforts are more advanced than those of the best civilian labs. Although the full extent of the agency's research remains unknown, the documents provided by Snowden suggest that the NSA is no closer to success than others in the scientific community.

https://www.cnet.com/tech/computing/ibm-new-53-qubit-quantum-computer-is-its-biggest-yet/

https://www.science.org/content/article/ibm-promises-1000-qubit-quantum-computer-milestone-2023

Development Roadmap

IBM **Quantum**



El universo post-cuántico (PQC)

Hay una buena posibilidad de que los ordenadores cuánticos sean capaces de descifrar el RSA-2048 en un plazo de cinco a diez años (se necesitan unos 20 Mqubits (sin CCE) en un ordenador universal para hacerlo).Algunos datos encriptados tienen una vida útil de más de diez años. Puede llevar diez años pasar a un nuevo esquema de cifrado, por lo que las empresas y los gobiernos están luchando para averiguar qué hacer.La mayoría de los cifrados que se usan hoy en día no son seguros en un mundo cuántico. Si alguien ha estado grabando una sesión de https, digamos, puede que no sea capaz de desencriptarla ahora, pero dentro de unos años, quién sabe.

opinión de la NIST

Cryptographic Algorithm	Type	Purpose	Impact from large-scale quantum computer
AES	Symmetric key	Encryption	Larger key sizes needed
SHA-2, SHA-3	----------	Hash functions	Larger output needed
RSA	Public key	Signatures, key establishment	No longer secure
ECDSA, ECDH (Elliptic Curve Cryptography)	Public key	Signatures, key exchange	No longer secure
DSA (Finite Field Cryptography)	Public key	Signatures, key exchange	No longer secure

NISTIR 8105

Impacto cuántico

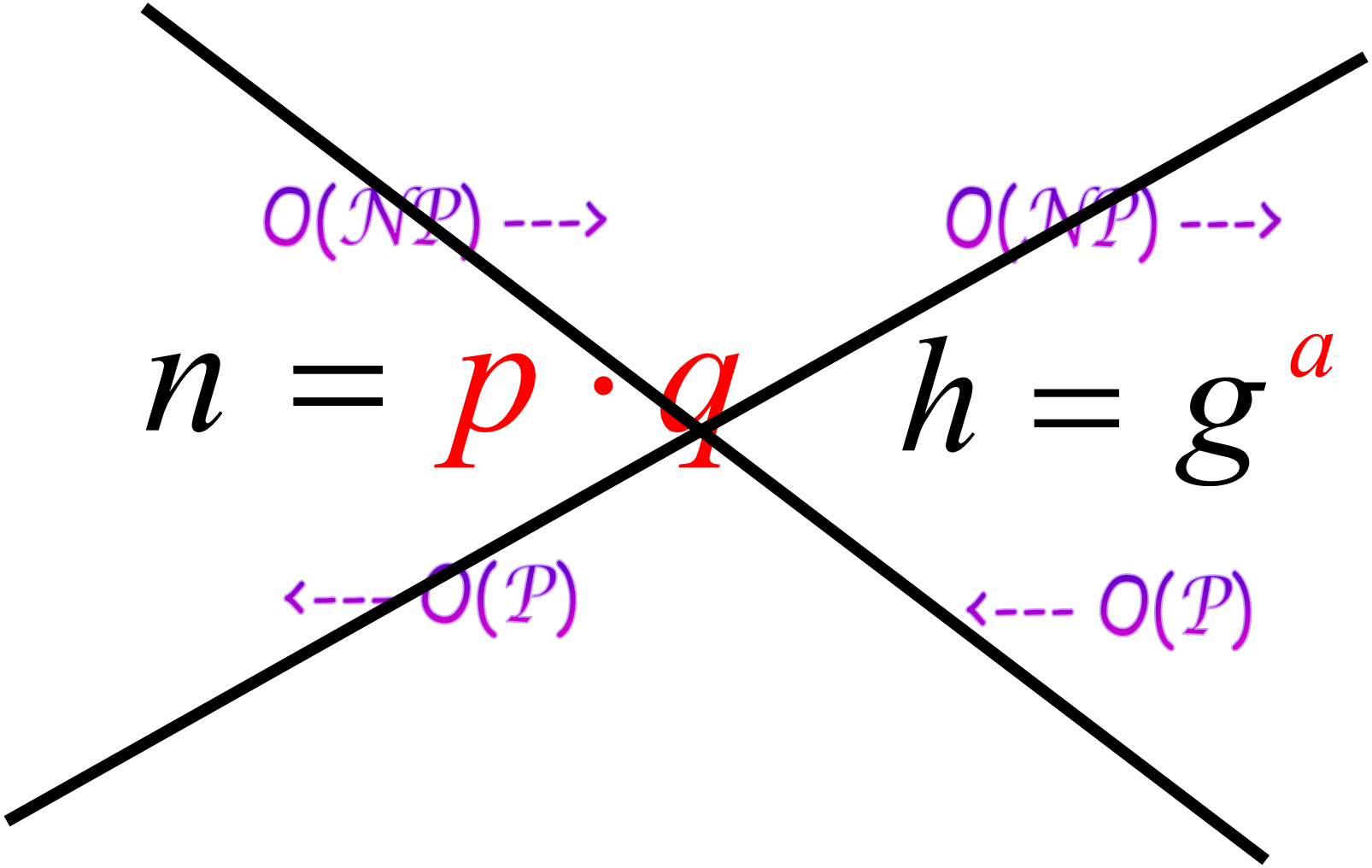
Name	Function	pre-quantum security level	post-quantum security level
Symmetric cryptography			
AES-128	block cipher	128	64
AES-256	block-cipher	256	128
Salsa20	stream cipher	256	128
GMAC	MAC	128	64
Poly1305	MAC	128	128
SHA-256	hash function	256	128
SHA-3	hash function	256	128
Public-key cryptography			
RSA-3072	encryption	128	broken
RSA-3072	signature	128	broken
DH-3072	key exchange	128	broken
DSA-3072	signature	128	broken
256-bit ECDH	key exchange	128	broken
256-bit ECDSA	signature	128	broken

Source: University of Illinois, Bernstein & Lange

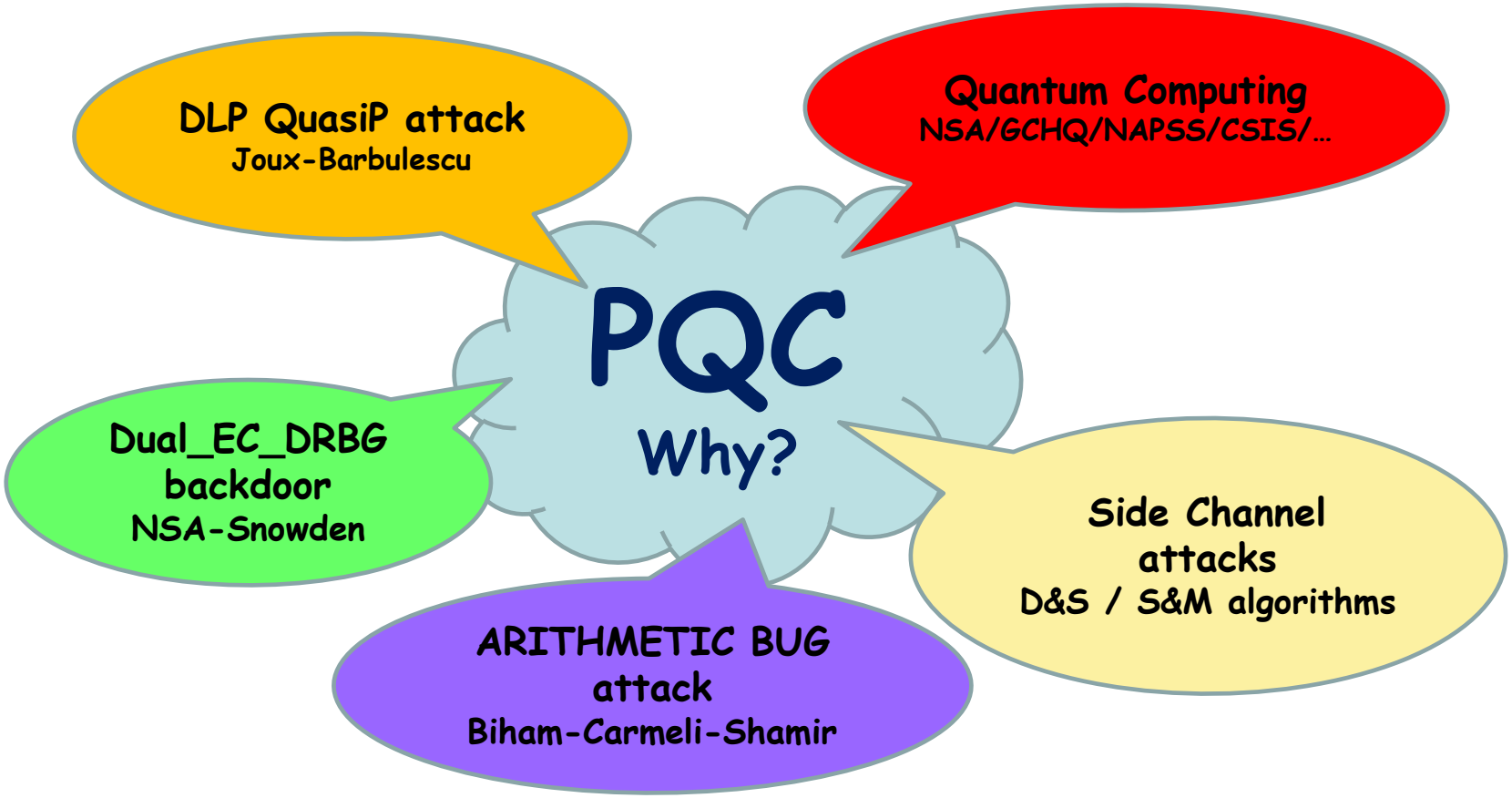
El algoritmo Grover reduce la complejidad cuadráticamente

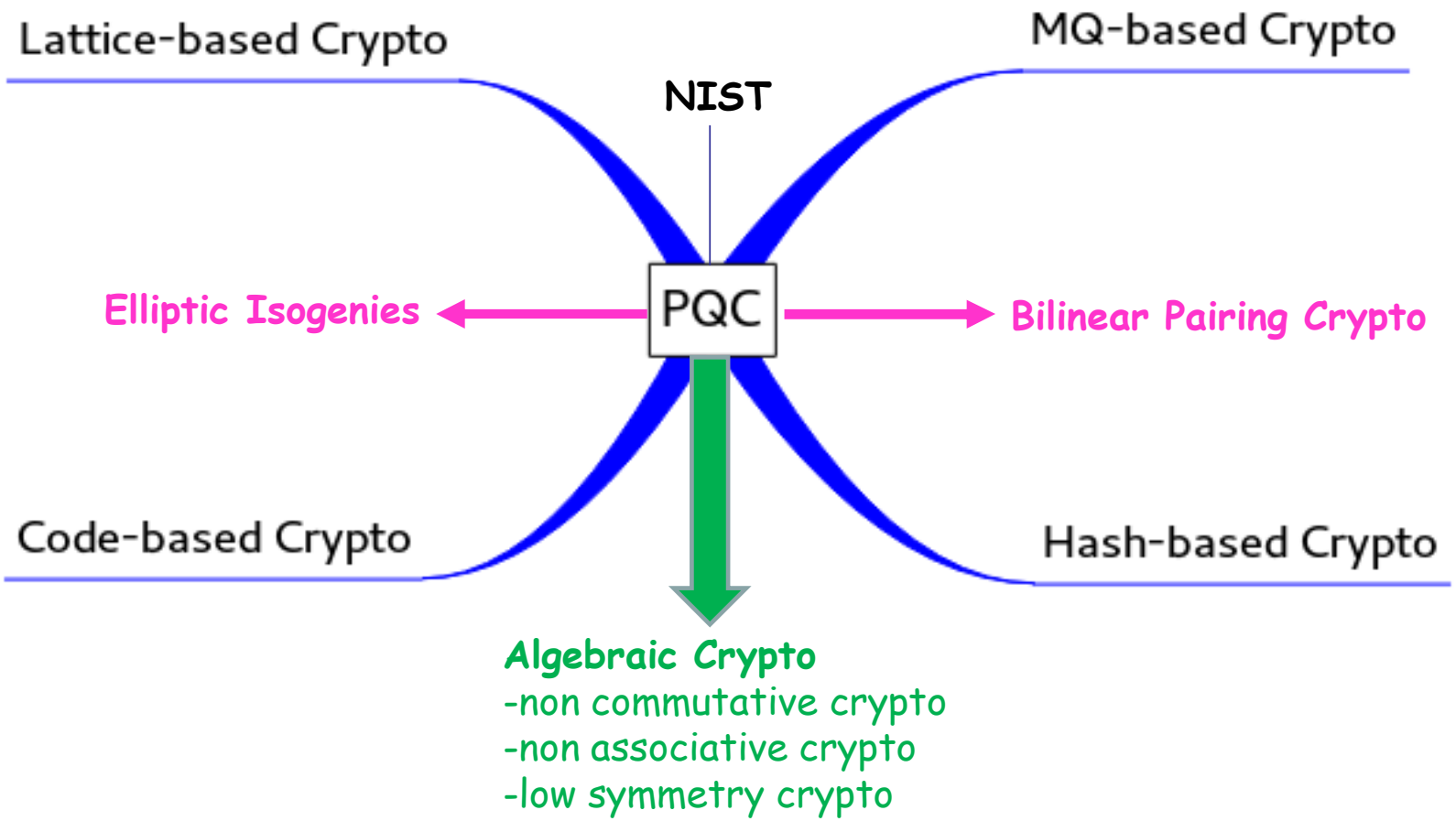
El algoritmo Shor destruye estos algoritmos

consecuencias inmediatas QC



Criptografía post cuántica (PQC)
convencional y alternativa

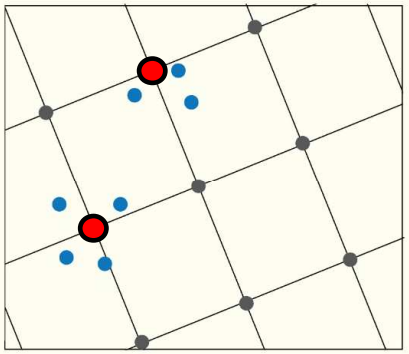

DLP QuasiP attack
Joux-Barbulescu
Quantum Computing
NSA/GCHQ/NAPSS/CSIS/...
PQC
Why?
Dual_EC_DRBG
backdoor
NSA-Snowden
Side Channel
attacks
D&S / S&M algorithms
ARITHMETIC BUG
attack
Biham-Carmeli-Shamir


Lattice-based Crypto
MQ-based Crypto
NIST
Elliptic Isogenies
PQC
Bilinear Pairing Crypto
Code-based Crypto
Hash-based Crypto
Algebraic Crypto
-non commutative crypto
-non associative crypto
-low symmetry crypto

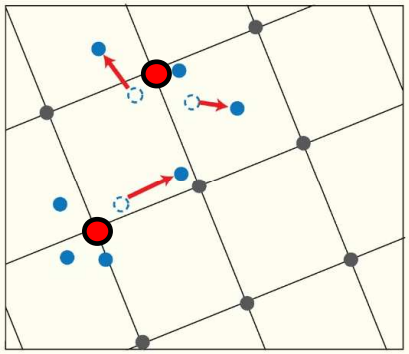
Lattice-Based Crypto

mensaje en claro
cifrado

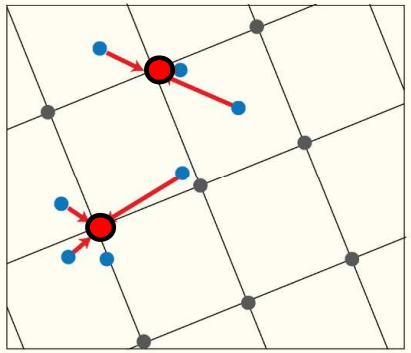
Lattice-based cryptography (for fully homomorphic encryption)



1. Encrypt
un cambio determinista



2. Add noise
+ un cambio aleatorio



3. Decrypt
recuperación

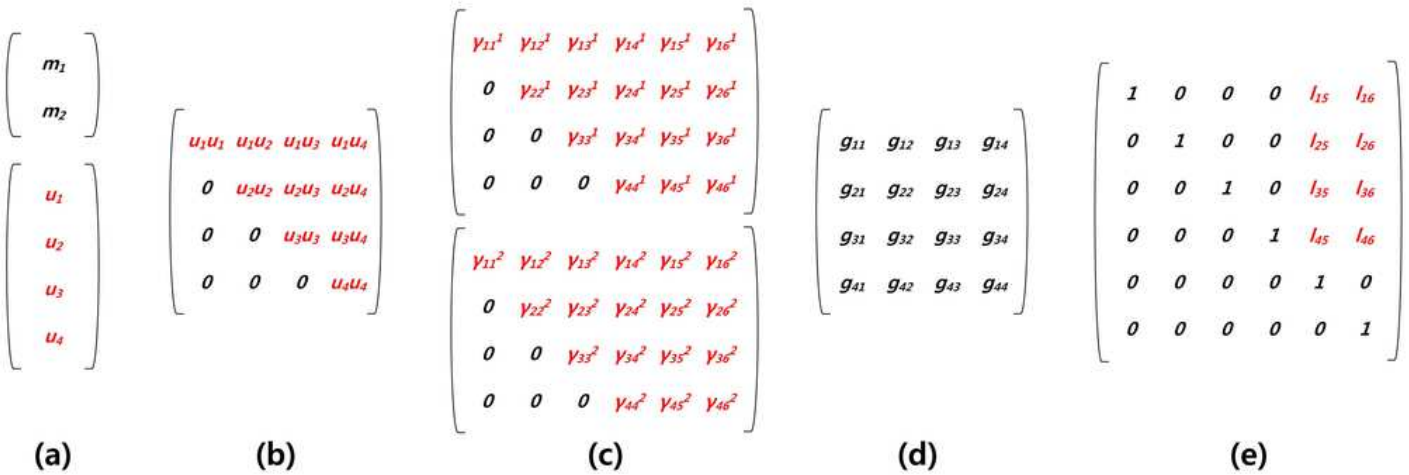
MQ Crypto

UNBALANCED OIL and VINEGAR - Patarin

- **IDEA:**

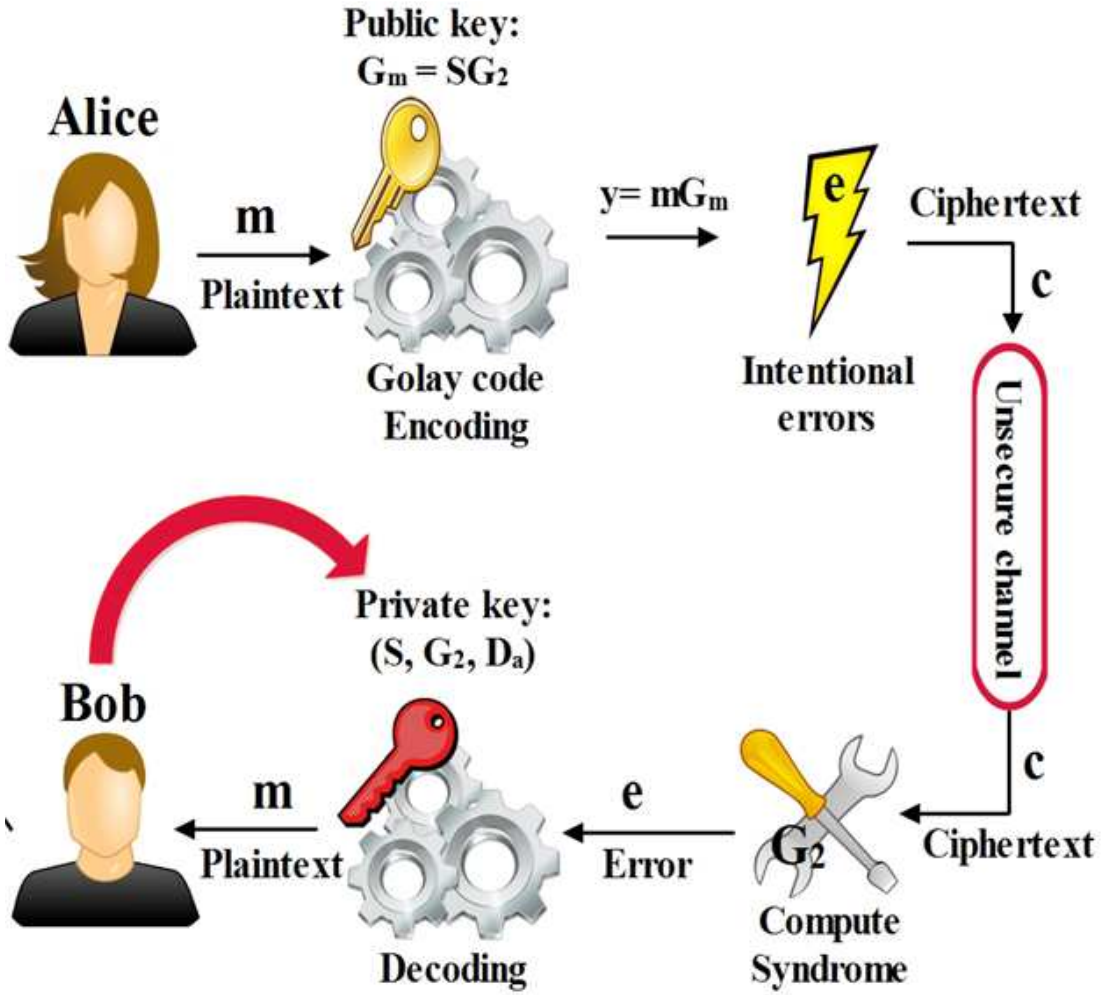
  Usar un sistema cuadrático modular con más variables (incógnitas) que ecuaciones… **(algo «imposible»….NP-COMPLETO)**

  Pero… generando una función TRAMPA de una vía que sí permita resolverlo



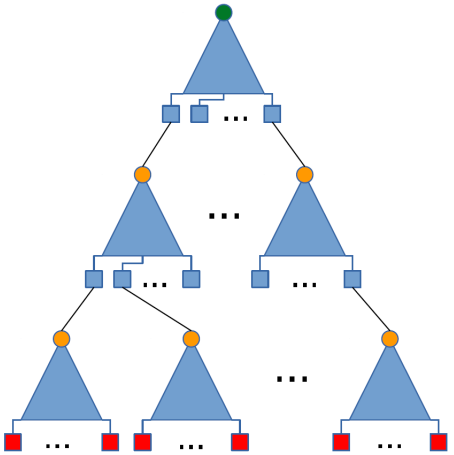
Code-based Crypto MC ELIECE

https://www.researchgate.net/profile/Amandeep-Bhatia/publication/328997272_McEliece_Cryptosystem_Based_On_Extended_Golay_Code/links/5e40d74a92851c7f7f2bc669/McEliece-Cryptosystem-Based-On-Extended-Golayode.pdf?origin=figuresDialog_download



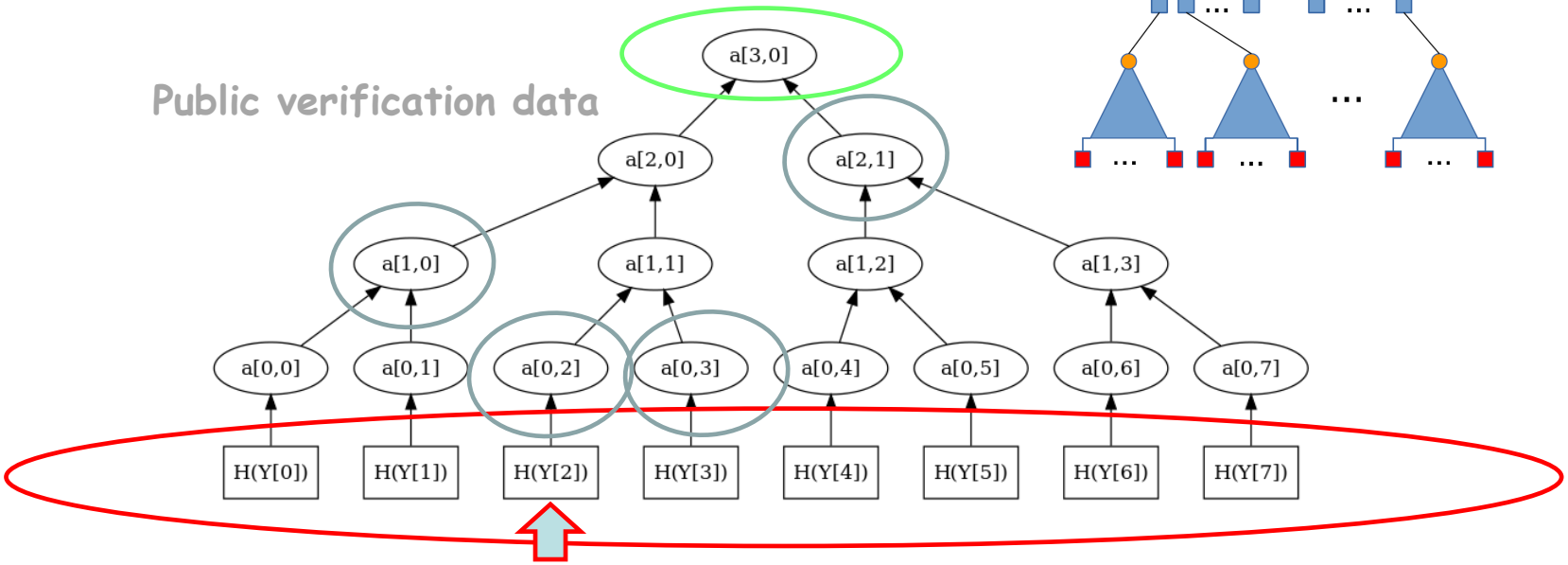
Hash-based Crypto

MERKLE HASH-TREE



Public signature key

Public verification data



Private signature key $[Y_0 \ldots Y_7]$ (one-time key)

Bilinear Pairing Crypto

$sea\ \ G_1\ un\ grupo\ aditivo\ cíclico\ de\ orden\ primo\ q$
$y\ P, Q \in G_1\ dos\ \ generadores$

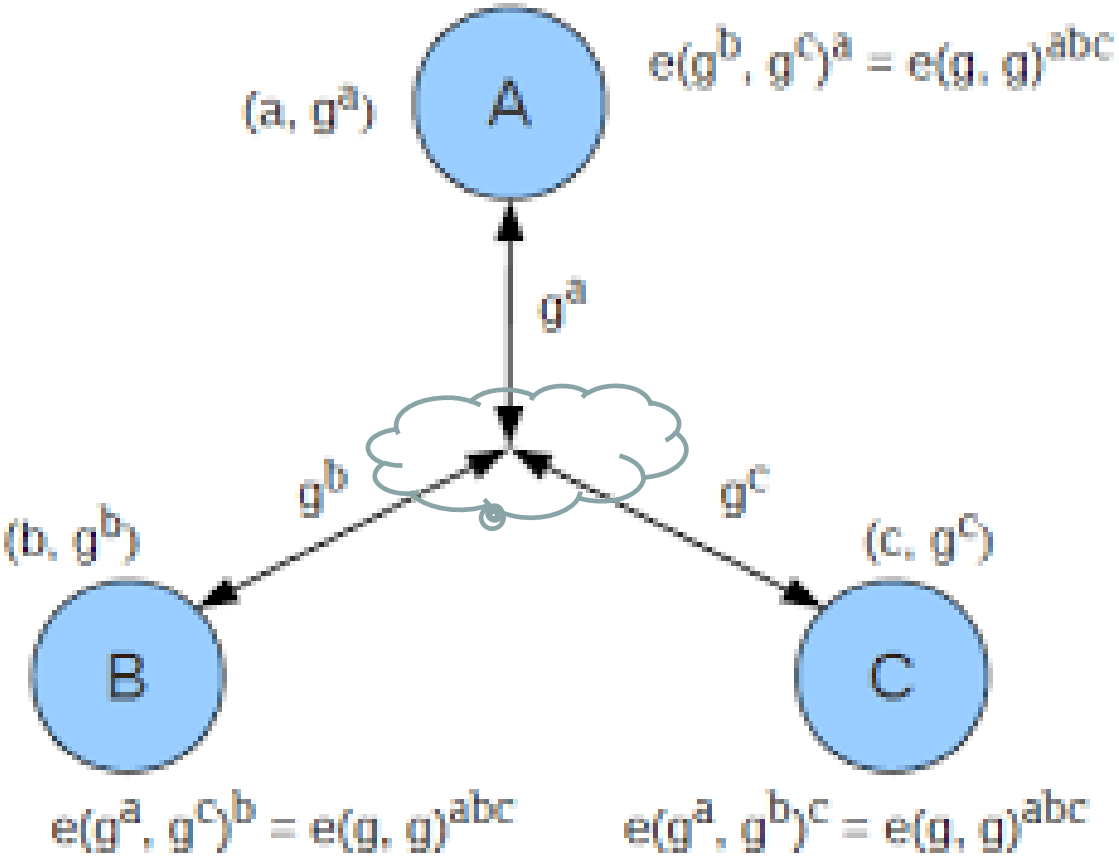
$\underline{Definir\ un\ mapa\ bilineal\ e}:$

$e: G_1\ x\ \ G_1 = G_2$

$donde\ G_2\ es\ un\ grupo\ cíclico\ multiplicativo$
$de\ orden\ primo\ q$

$$\forall\ P, Q\ \in G_1\ \ , \forall a, b\ \in \mathbb{Z}_q{}^*$$
$$e(aP, bQ) = e(P, Q)^{ab} \in G_2$$

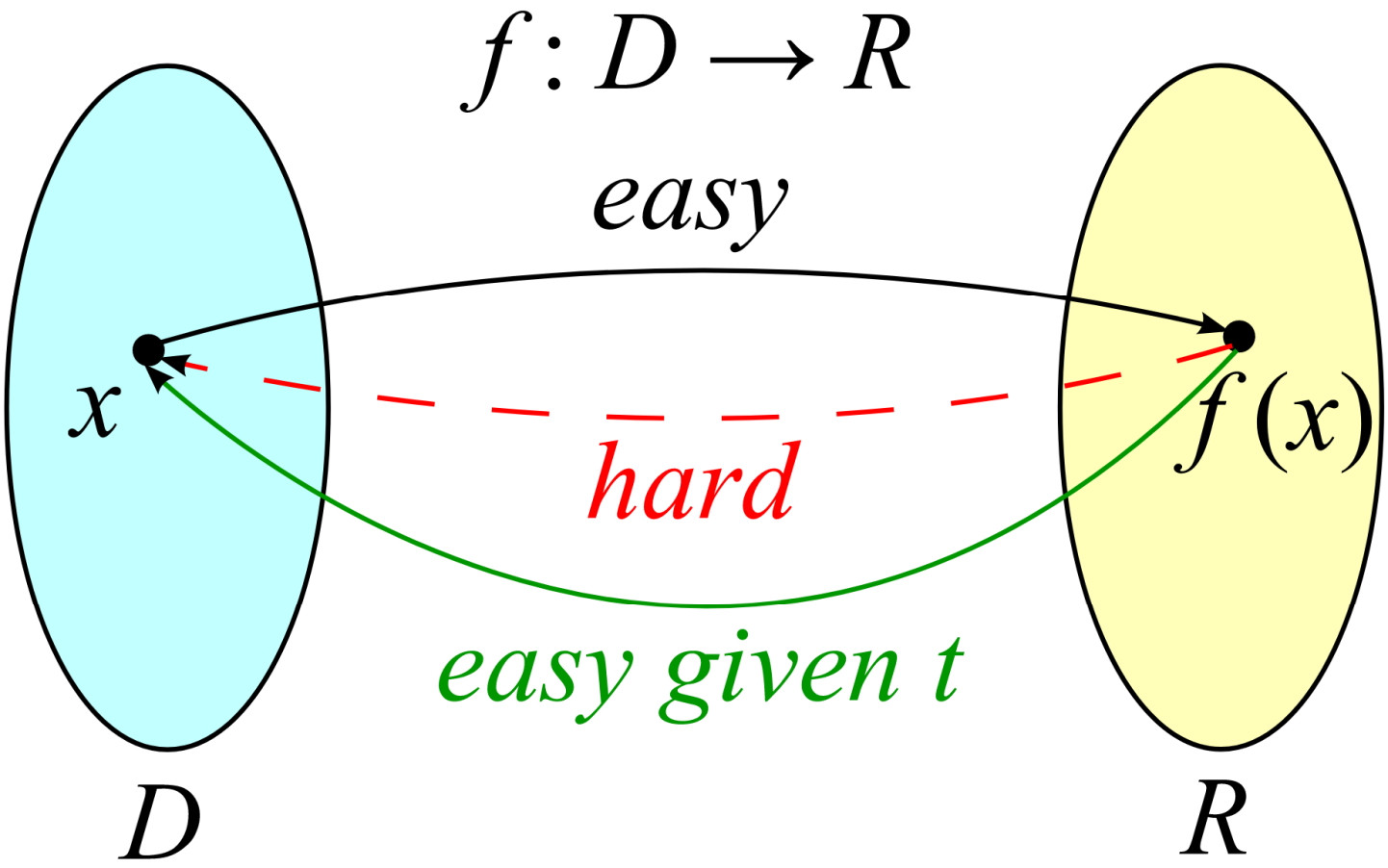
Tripartite one-pass DH (Joux)



Métodos PQC	Características	Propósito	Ventajas	Desventajas	Ejemplos
Criptografía de ecuaciones cuadráticas y multivariantes	Basada en polinomios de múltiples variables en un campo finito (problema de isomorfismo de polinomios).	Firmas digitales	• Firmar y Verificar es muy rápido. • Producen firmas digitales más cortas.	• Parecen ser una buena alternativa a los esquemas de hash. • Requiere la utilización de tamaños muy grandes de clave. • No se conoce a fondo la seguridad.	Unbalanced Oil & Vinegar
Criptografía basada en Hash	Basada en funciones que entregan un resumen de los bits del mensaje	Firmas digitales	• Se consideran suficientemente sólidos para firmas digitales postcuánticas al utilizar Arboles de Merkle.	• Requiere mucha infraestructura por lo tanto no es un mecanismo rápido. • No existen esquemas de cifrado de clave pública, basados en funciones de hash • Hay que mantener recuerdo de todas las claves de un solo uso que son utilizadas en el proceso.	Árboles de Merkle como XMSS y SPHINCS (con claves de 256 bits)
Criptografía basada en código	Basada en códigos de detección y corrección de errores que utilizan algebra lineal (Códigos Goppa)	Cifrado y Descifrado	• Esquema de cifrado muy eficiente. • Parecen ser una de las alternativas postcuánticas más fiables.	• Requiere la utilización de tamaños muy grandes de clave. • Hay variantes que permiten implementaciones en hardware.	Cifrado McEliece y Criptosistema de Niederreiter

Métodos PQC	Características	Propósito	Ventajas	Desventajas	Ejemplos
Criptografía isogenética de la curva elíptica supersingular	Basada en una aplicación racional entre dos curvas elípticas que preserva la estructura de grupo asociado (homomorfismo de grupos).	Cifrado, Firma y Hashes	• No se conocen algoritmos que puedan romper el problema base. • Crea un reemplazo de Diffie Hellman con secreto	• No se conocen hasta ahora.	SIDH
Criptografía basada en retículos	Basada en problemas matemáticos de retículos. Trabaja con ecuaciones diofánticas de gran dimensión.	Cifrado, Firma y Hashes	• No existen algoritmos conocidos capaces de resolverlos ni siquiera con ordenadores cuánticos.	• No se conoce a fondo la seguridad. • Hay que hacer modificaciones que presenten implementaciones eficientes. • Requiere más investigación.	NTRU4 y NTRUMLS
Criptografía basada en emparejamientos	Basada en mapas bilineales donde G1 es una curva elíptica y G2 un campo finito	Firmas digitales	• El uso de funciones bilineales reduce un problema NP en otro de clase P • No es necesario que participe la Autoridad Certificante.	• No se conocen hasta ahora.	BLS Boneh-Lynn-Shacham IBC (Criptografía basada en identidad)

Criptografía post cuántica (PQC)
algunos ejemplos basados en álgebra abstracta


$f : D \to R$
easy
x
hard
$f(x)$
easy given t
D
R

Criptografía asimétrica post-cuántica basada en álgebra no conmutativa:
un cambio de plataformas...

- grupos, semigrupos, monoides, quasigrupos y anillos **no conmutativos**
- sin riesgo a la vista de sufrir **ataques cuánticos**
- A mayor asimetría interna, **mayor seguridad**
- aritmética modular reducida **sin bibliotecas de precisión extendida**

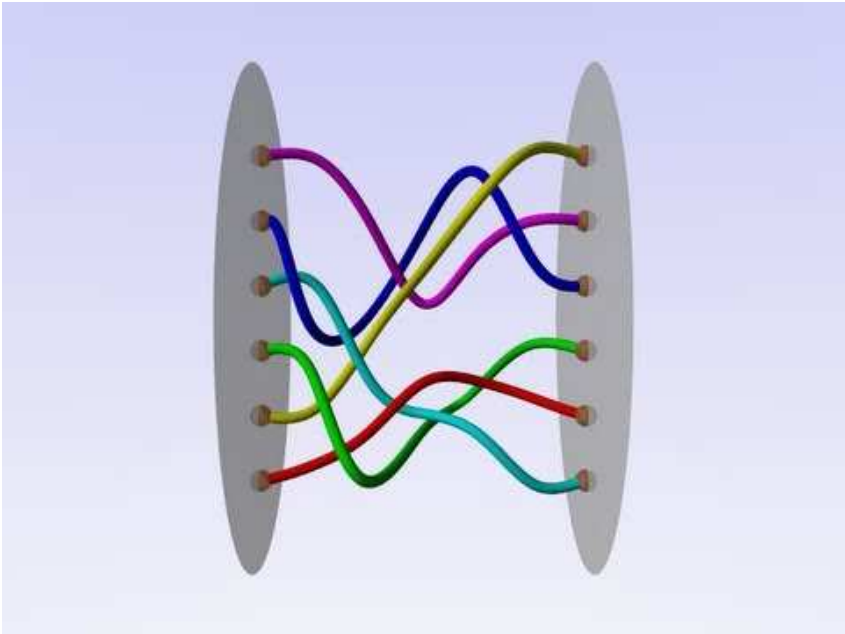
OWTF

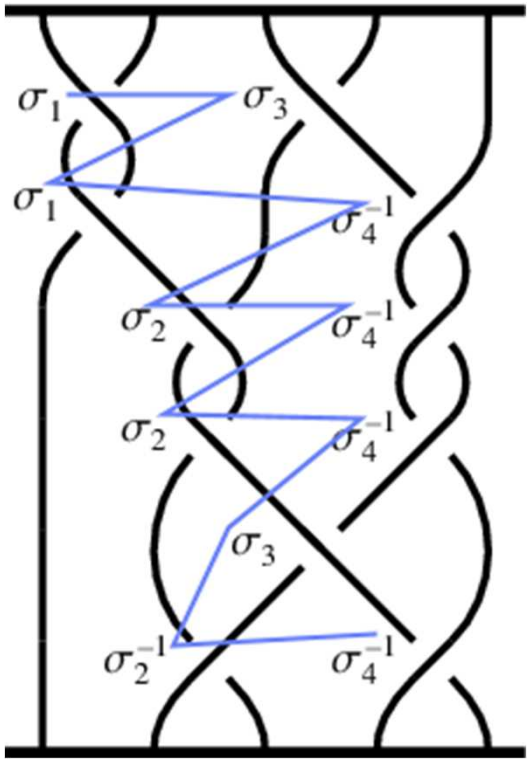
Como función trampa de una vía se elige por ejemplo el problema de la **búsqueda de un elemento z en un subgrupo,** en una instancia $\mathcal{NP}$ del problema del logaritmo discreto generalizado (GDLP), derivado del problema de búsqueda de un conjugador ($y = z^{-1} x z$)

PROBLEMA GSDP

$$Sea\ G\ un\ grupo\ no\ conmutativo:$$
$$dados\ (x,y) \in G^2, (m,n) \in Z^2,$$
$$S \subset G, hallar\ z \in S\ \ tal\ que$$
$$y = z^m\ x\ \ z^n$$

Criptografía de Trenzas

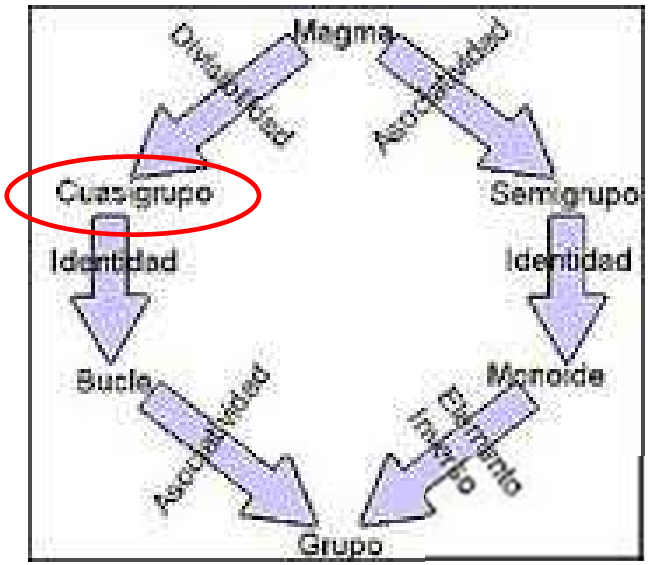




$Pública \quad \sigma_B = \sigma_x \sigma_A \, \sigma_x^{-1}$

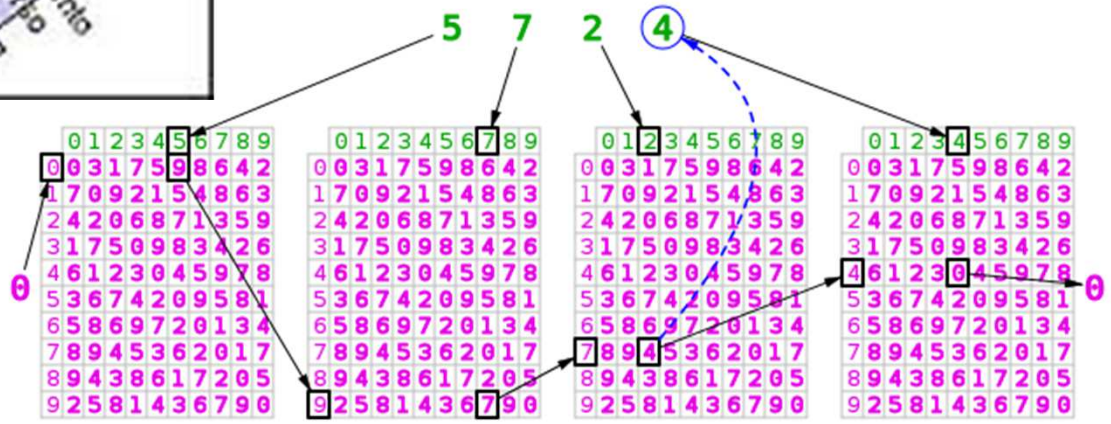
$Privada \quad \sigma_x \quad (CSP)$

Cuasigrupos



$z = xy$

x \ y	a	b	c	d	e	f
a	a	b	c	d	e	f
b	b	a	d	c	f	e
c	c	e	a	f	b	d
d	d	f	b	e	a	c
e	e	c	f	a	d	b
f	f	d	e	b	c	a



LD-Magmas (tablas Laver)

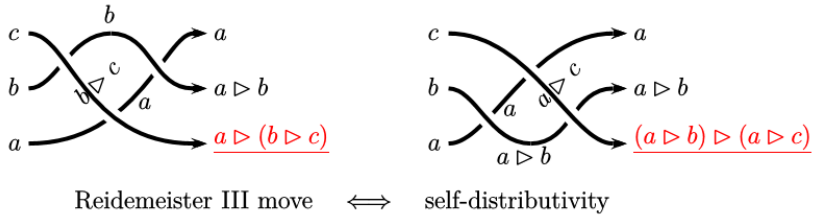
Un ejemplo de LD-Magma son las Tablas LAVER representables por $(A_n, *)$: $A_n \Rightarrow \{1,2,3,\ldots,2^n\}$

$$(x,y,z) \in A_n^3$$

$$(LD\ def)\ * \Rightarrow\ x * (y*z) = (x*y) * (x*z)$$

Junto a la condición inicial: $x * 1 = x + 1 \pmod{2^n}$

Son estructuras no asociativas, no conmutativas y sin inversa. También las trenzas poseen estas propiedades.



Reidemeister III move $\Longleftrightarrow$ self-distributivity

A_0	1
1	1

A_1	1	2
1	2	2
2	1	2

A_2	1	2	3	4
1	2	4	2	4
2	3	4	3	4
3	4	4	4	4
4	1	2	3	4

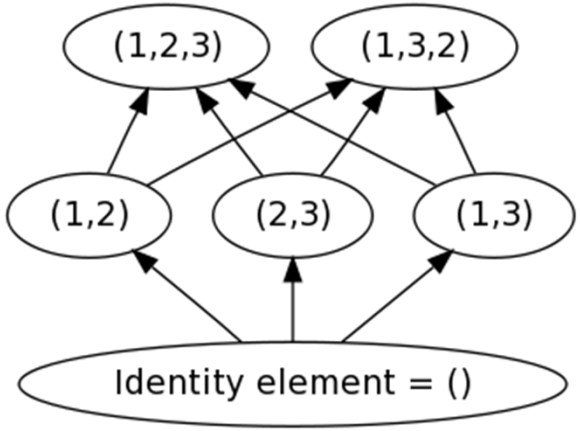
A_3	1	2	3	4	5	6	7	8
1	2	4	6	8	2	4	6	8
2	3	4	7	8	3	4	7	8
3	4	8	4	8	4	8	4	8
4	5	6	7	8	5	6	7	8
5	6	8	6	8	6	8	6	8
6	7	8	7	8	7	8	7	8
7	8	8	8	8	8	8	8	8
8	1	2	3	4	5	6	7	8

A_4	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	2	12	14	16	2	12	14	16	2	12	14	16	2	12	14	16
2	3	12	15	16	3	12	15	16	3	12	15	16	3	12	15	16
3	4	8	12	16	4	8	12	16	4	8	12	16	4	8	12	16
4	5	6	7	8	13	14	15	16	5	6	7	8	13	14	15	16
5	6	8	14	16	6	8	14	16	6	8	14	16	6	8	14	16
6	7	8	15	16	7	8	15	16	7	8	15	16	7	8	15	16
7	8	16	8	16	8	16	8	16	8	16	8	16	8	16	8	16
8	9	10	11	12	13	14	15	16	9	10	11	12	13	14	15	16
9	10	12	14	16	10	12	14	16	10	12	14	16	10	12	14	16
10	11	12	15	16	11	12	15	16	11	12	15	16	11	12	15	16
11	12	16	12	16	12	16	12	16	12	16	12	16	12	16	12	16
12	13	14	15	16	13	14	15	16	13	14	15	16	13	14	15	16
13	14	16	14	16	14	16	14	16	14	16	14	16	14	16	14	16
14	15	16	15	16	15	16	15	16	15	16	15	16	15	16	15	16
15	16	16	16	16	16	16	16	16	16	16	16	16	16	16	16	16
16	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

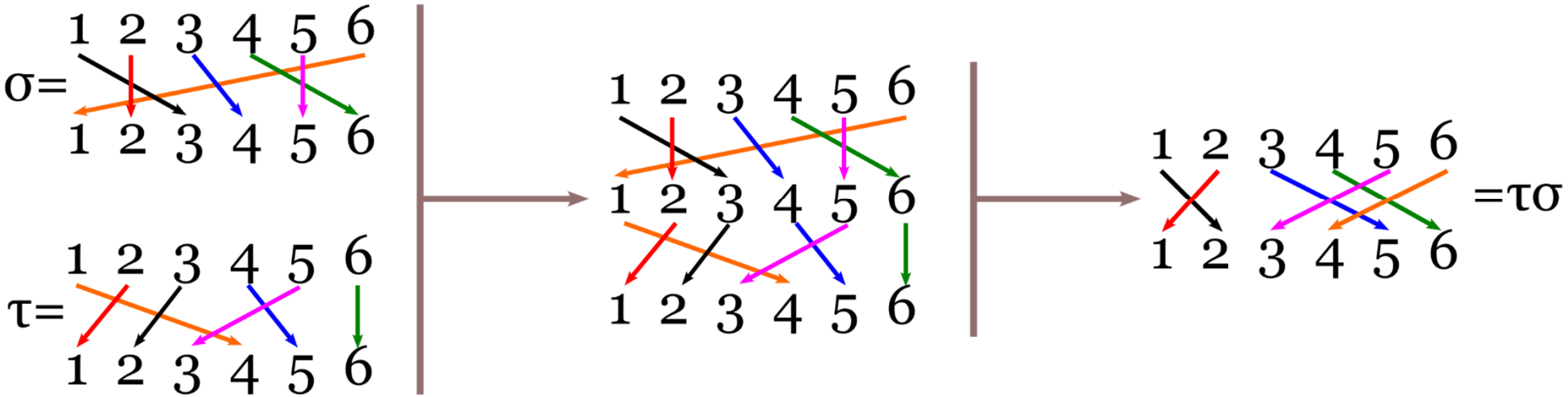
Grupos NC: permutaciones

∘	(1)	(123)	(132)	(12)	(13)	(23)
(1)	(1)	(123)	(132)	(12)	(13)	(23)
(123)	(123)	(132)	(1)	(23)	(12)	(13)
(132)	(132)	(1)	(123)	(13)	(23)	(12)
(12)	(12)	(13)	(23)	(1)	(123)	(132)
(13)	(13)	(23)	(12)	(132)	(1)	(123)
(23)	(23)	(12)	(13)	(123)	(132)	(1)

Private σ_{ALICE}
Public $(\varepsilon , \pi_{ALICE} = \sigma_{ALICE} \ \varepsilon \ \sigma^{-1}_{ALICE})$
Crypto generalized ElGamal
Security CSP



composición de permutaciones



$(231645)^1 = (231645)$

$(231645)^2 = (524631)$

$(231645)^3 = (261435)$

...

$O(P)$ -->

$(231645)^x = (614235)$

<-- $O(NP)$

Operando con estructuras matriciales:

Generación de claves públicas y privadas

Preparación (TTP)
Elementos públicos $P \in_R M_8$ *y* $G \in_R M_8$
Elementos públicos $(m, n) \in_R \mathbb{Z}_{251}^2$ *donde* $m \neq n$ *y ambos* >2

Claves Privadas
ALICE: $D_A=(\lambda_1...\lambda_8) \in_R \mathbb{Z}_{251}^8$ *y* $A=P \cdot D_A \cdot P^{-1}$
BOB: $D_B=(\lambda_1...\lambda_8) \in_R \mathbb{Z}_{251}^8$ *y* $B=P \cdot D_B \cdot P^{-1}$

Claves Públicas
ALICE: $A'=A^m \cdot G \cdot A^n$
BOB: $B'=B^m \cdot G \cdot B^n$

OBS: Deducir la clave privada a partir de la pública requiere resolver el problema GSDP.
Las potencias de claves privadas conmutan.

1. Intercambio de claves (Diffie-Hellman generalizado)

ALICE

$(k1, k2) \in_R [2,z]^2$

$T_A = A^{k1}\ G\ A^{k2}$

$K = A^{k1}\ T_B\ A^{k2}$

$(r1, r2) \in_R [2,z]^2$

$T_B = B^{r1}\ G\ B^{r2}$

$K = B^{r1}\ T_A\ B^{r2}$

BOB

$K = A^{k1}T_B A^{k2} = A^{k1}(B^{r1}G\ B^{r2})A^{k2} = B^{r1}(A^{k1}G\ A^{k2})B^{r2} = B^{r1}\ T_A\ B^{r2}$

2. Transporte de claves (Baumslag generalizado)

ALICE

Elige K $\in_R M_8$

$(k1, k2) \in_R [2,z]^2$

$T_A = A^{k1}\ \mathbf{K}\ A^{k2}$

$S = A^{-k1}\ T_B\ A^{-k2}$

$(r1, r2) \in_R [2,z]^2$

$T_B = B^{r1}\ T_A\ B^{r2}$

$\mathbf{K} = B^{-r1}\ S\ B^{-r2}$

BOB

$$\mathbf{K} = B^{-r1}\ S\ B^{-r2} = B^{-r1}(A^{-k1}\ T_B\ A^{-k2})B^{-r2}$$
$$= A^{-k1}(B^{-r1}(B^{r1}\ T_A\ B^{r2})B^{-r2})A^{-k2} = A^{-k1}T_A\ A^{-k2} =$$
$$= A^{-k1}(A^{k1}\ \mathbf{K}\ A^{k2})\ A^{-k2} = \mathbf{K}$$

3. Cifrado (ElGamal generalizado)

ALICE

Claves Privadas
ALICE: $D_A=(\lambda_1...\lambda_8) \in_R \mathbb{Z}_{251}^8$ y $A=P \cdot D_A \cdot P^{-1}$
BOB: $D_B=(\lambda_1...\lambda_8) \in_R \mathbb{Z}_{251}^8$ y $B=P \cdot D_B \cdot P^{-1}<$

Claves Públicas (G, m,n)
ALICE: $A'=A^m \cdot G \cdot A^n$
BOB: $B'=B^m \cdot G \cdot B^n$

Elige $M_{msg} \in M_8$ y $K_{sesión} \in_R P_8$ (secreta)

$$C = (y_1, y_2) = (K^m\ G\ K^n\ ,\ M\ (K^m\ B'\ K^n)\ )$$

$$M = y_2\ (B^m\ y_1\ B^n)^{-1}$$

BOB

$$M = y_2\ (B^m\ y_1\ B^n)^{-1} = M\ (K^m\ B'\ K^n)\ (B^m\ y_1\ B^n)^{-1} =$$
$$= M\ (K^m\ B^m) G\ B^n K^n)\ (B^m\ y_1\ B^n)^{-1} =$$
$$= M\ (B^m (K^m G\ K^n) B^n)\ (B^m\ y_1\ B^n)^{-1} =$$
$$= M (B^m\ y_1\ B^n)\ (B^m\ y_1\ B^n)^{-1} = M$$

4. Firma Digital

Clave Privada
ALICE: $D_A=(\lambda_1...\lambda_8) \in_R \mathbb{Z}_{251}^8$ y $A=P \cdot D_A \cdot P^{-1}$

Se define: Hashing $H(msg) \in_R P_8$ donde $msg \in \{0,1\}^n$

ALICE

ALICE define: $L \in_R P_8$ (privada) y $(m, n) \in_R [2,z]^2$ (privados)

ALICE define: $A' = A^m \, L \, A^n$ (público)

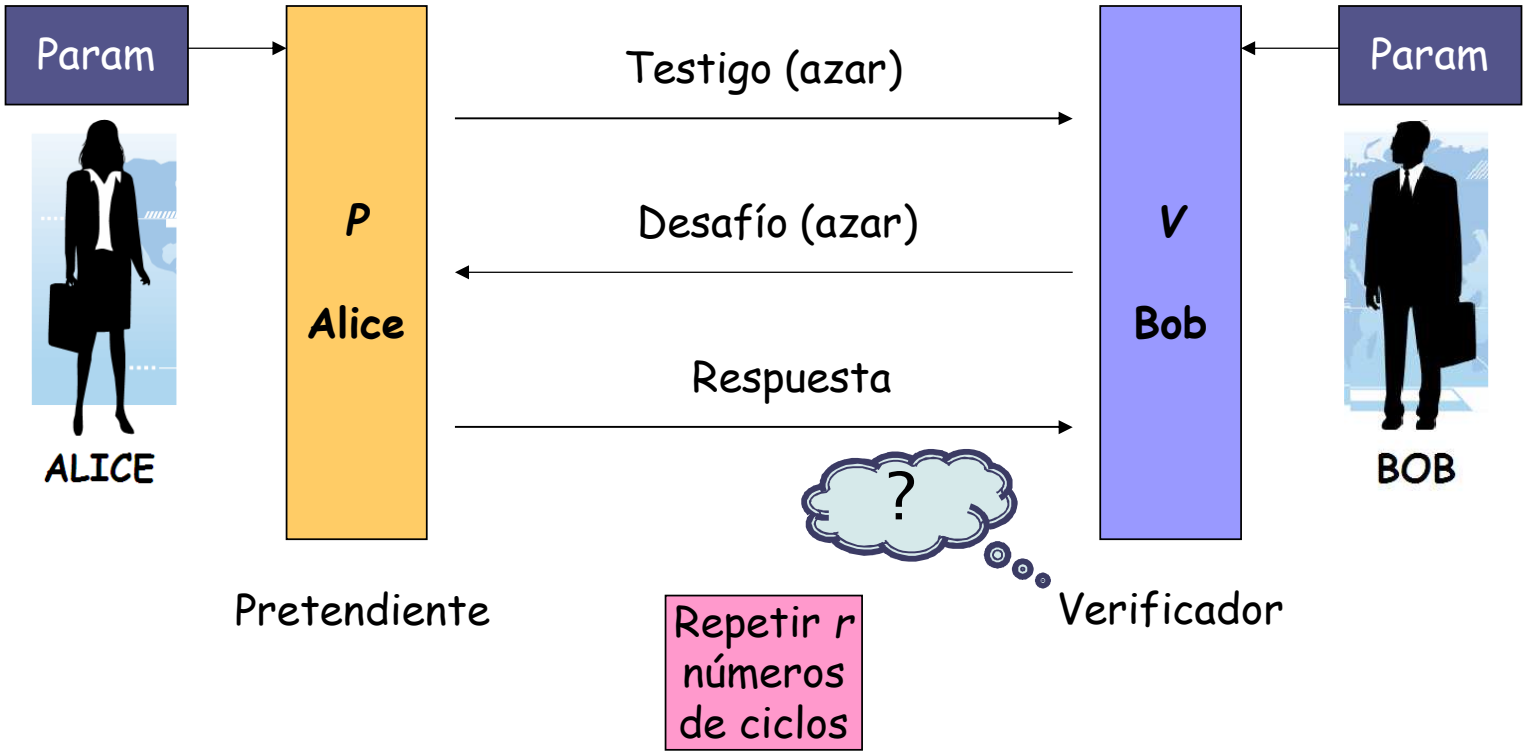
$$F = A^{-n} \, L^{-1} \, H(msg) \, A^{-m}$$

$$H_{recup}(msg) = F \, A'$$

$$H_{recup}(msg) = F \, A' = (A^{-n} \, L^{-1} \, H(msg) \, A^{-m})(A^m \, L \, A^n) =$$
$$= H(msg) \, (A^{-n} \, L^{-1} \, A^{-m})(A^m \, L \, A^n) =$$
$$= H(msg)$$

Se comparan H_{recup} *vs* H_{recalc}

Prueba de Identidad Interactiva



Protocolo ZKP de Identidad

- Caso especial de las pruebas interactivas
- Las pruebas de conocimiento cero ofrecen una vía de probar conocimiento a cualquier entidad sin transferirle ningun dato adicional acerca de ese conocimiento.

Un solo bit del secreto que se filtre invalida la propiedad ZK

ZKP

ALICE
pretendiente

Claves Privadas
ALICE: $D_A=(\lambda_1...\lambda_8) \in_R \mathbb{Z}_{251}^8$ y $A=P \cdot D_A \cdot P^{-1}$
BOB: $D_B=(\lambda_1...\lambda_8) \in_R \mathbb{Z}_{251}^8$ y $B=P \cdot D_B \cdot P^{-1}$

Claves Públicas (G, m,n)
ALICE: $A'=A^m \cdot G \cdot A^n$
BOB: $B'=B^m \cdot G \cdot B^n$

BOB
verificador

$k_{secreto} \in_R [2,z]$

$S = A^k B' A^{-m}$ → testigo → S

$b_{bit} \in_R [0,1]$

desafío → (b, Q)

Si b=0
$H \in_R M_8$
$Q = B^m H B^n$

Si b=1
$Q = B^m S A' B^n$

Si b=0
$R = S^{-m} Q S^{-n}$

Si b=1
$R = A^{-k} Q A^{-n}$

respuesta → R

verificación

Si b=0
$S^m R S^n = Q$?

Si b=1
$B^{-m} R B^{-n} = B'G$?

Iterar r-veces

$p_{aceptac\ fraude} = (1/2)^r$

Seguridad de los protocolos

$|M_{8x8\ (mod\ 251)}| = 251^{8^2} =$

37941821347055989703405920631602419334780075492489875492312621532472379648717156420169788319206974069849682809998818454484652557491978888857950886260160 01 $\sim 10^{153.579}$

(=100%)

$|GL(8,Z_{251})| = |M_8| = 251^{8^2} . (1-1/251).(1-1/251^2).(1-1/251^3).(1-1/251^4).(1-1/251^5).(1-1/251^6).(1-1/251^7).(1-1/251^8) =$

37790056470672143375523887777615580628893396182359572719226032510348647340472613948040534368328922861846053662190855900649834361785937500000000000000000000 $\sim 10^{153.577}$

(~ 99.6%)

$|D_8| = |P_{8\ (P)}| = 249.248 .247.246.245.244.243.242 =$

1319048117869914432 0 $\sim 10^{19.1203} \sim 2^{63.5161}$ (~64 **bits**)

Potencias matriciales (ciclos multiplicativos)

- A cada matriz en **$GL(8,Z_{251})$** le corresponde un polinomio característico mónico grado 8 módulo 251.
- Sus características determinan la longitud de los ciclos multiplicativos.
- Polinomios de grado 8 módulo 251

$$N_{tot}(p,m) = p^m = 251^8 = 1575396121181425 2001 \sim 10^{19.1974}$$

(=100%)

- Polinomios irreducibles en **F_{p^m}** cuyo **$ord_{251}()$** es divisor de $p^m - 1$

$$N_p(m) = \frac{1}{m}\sum_{d|m} \mu(d) p^{m/d} = 196924515098064 0750 \sim 10^{18.2943}$$

(= 87.5%)

- El orden multiplicativo de un polinomio irreducible elegido al azar en F_{p^m} (divisor de $p^m - 1$) es cercano al máximo posible. Para un campo primo **F_p** es del orden de $\varphi(p)$ (*Luca-Shparlinsky, Average multiplicative order of elements module n*).
- Polinomios primitivos en F_{p^m} cuyo **$ord_{251}(f)$** es $p^m - 1$

$$M_p(m) = \frac{\varphi(p^m-1)}{m} = 41974936335360 0000 \sim 10^{17.6230}$$

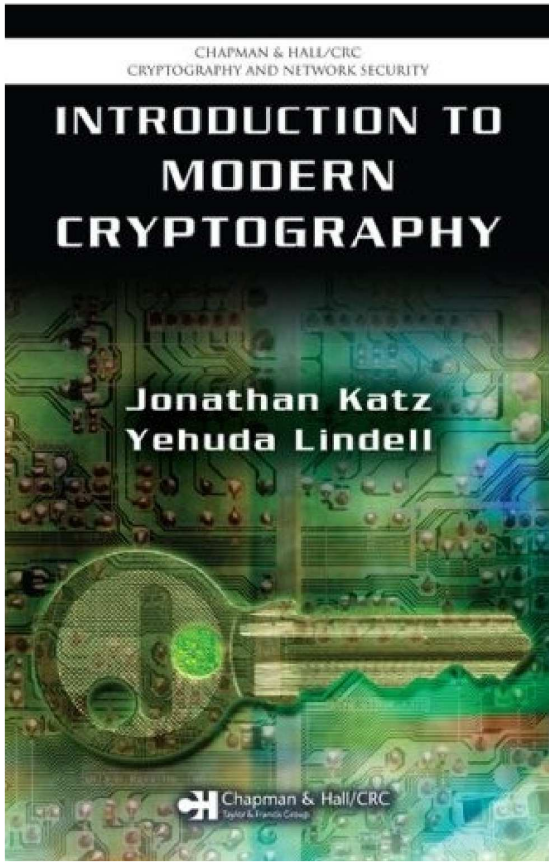
(~ 2.7%)

TWEAK (*R-propping*)

Pasar de aritmética matricial en campo numérico $(Z_p,\oplus,\odot)$ a operaciones en anillo polinómico de matrices $(Z_p[x],\boxplus,\boxdot)$.

Un nuevo paradigma en la criptografía:

SEGURIDAD DEMOSTRABLE



IND/NM-CPA

Indistinguishable /Non-Malleable Choosen Plaintext Attack
(SEGURIDAD SEMÁNTICA)

IND/NM-CCA1

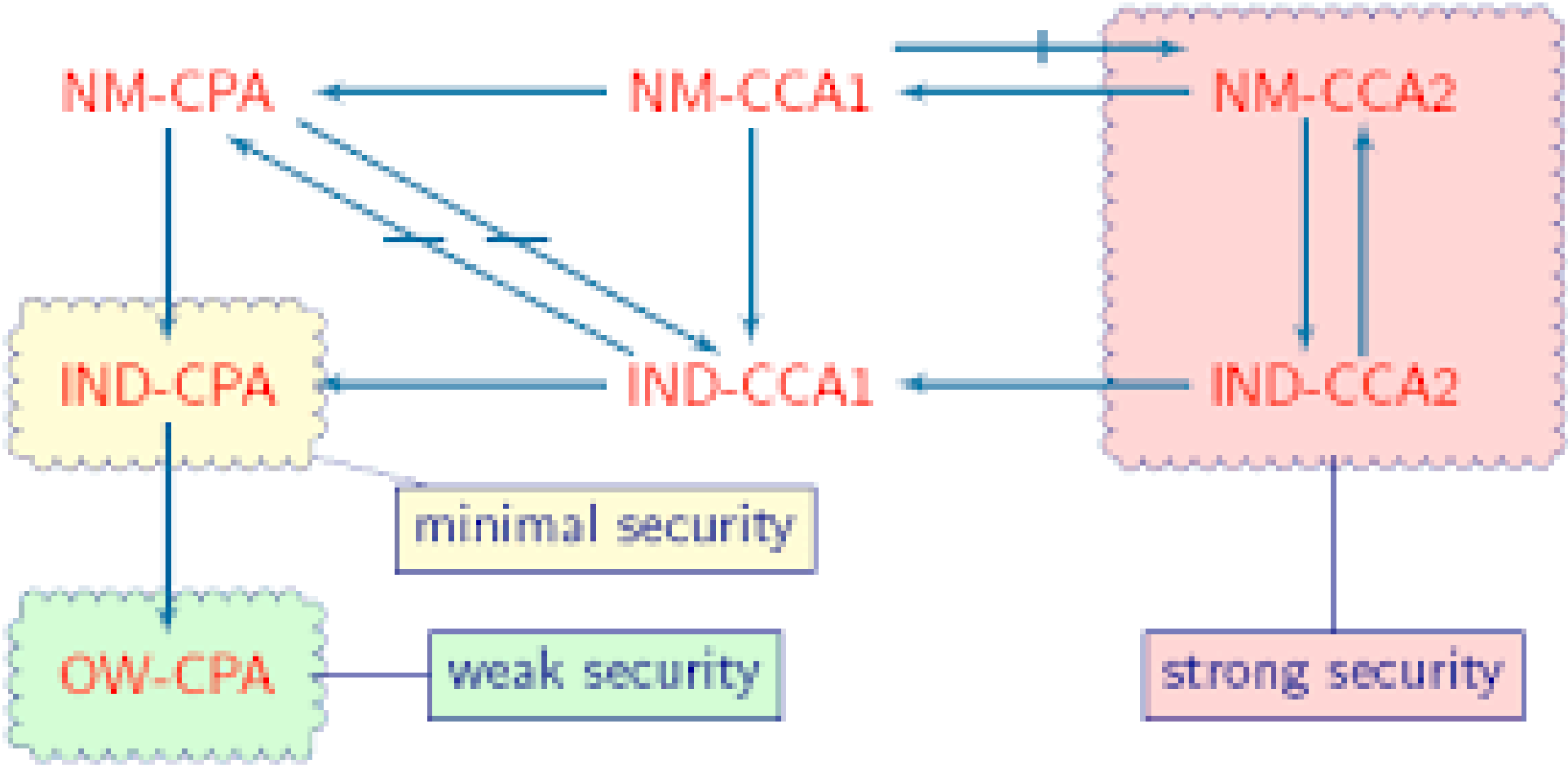
Indistinguishable /Non-Malleable Choosen Ciphertext Attack

IND/NM-CCA2

Indistinguishable /Non-Malleable Adaptative Choosen

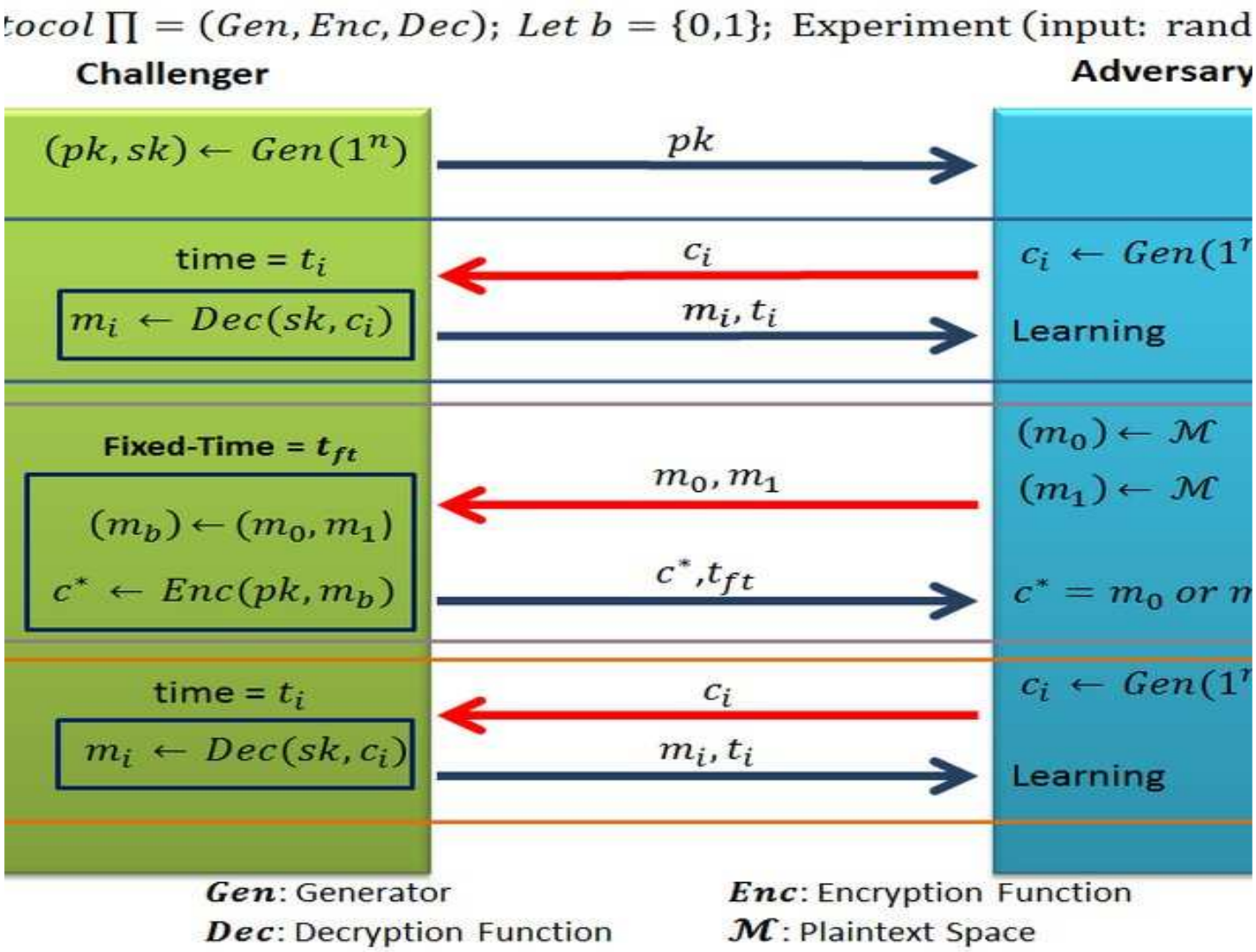
Ciphertext Attack

en grado de seguridad creciente:
IND-CPA < IND-CCA1 < NM-CCA2 = IND-CCA2


NM-CPA
NM-CCA1
NM-CCA2
IND-CPA
IND-CCA1
IND-CCA2
minimal security
OW-CPA
weak security
strong security

Los niveles IND se plantean como un juego interactivo entre un desafiante y un adversario que debe quebrar la seguridad semántica de un cifrado

(la quiebra si es capaz de distinguir si un cifrado corresponde a un determinado mensaje, dados dos de ellos de igual longitud y que él generó a voluntad)


tocol $\prod = (Gen, Enc, Dec)$; Let $b = \{0,1\}$; Experiment (input: rand
Challenger
Adversary
$(pk, sk) \leftarrow Gen(1^n)$
pk
time = t_i
$m_i \leftarrow Dec(sk, c_i)$
c_i
m_i, t_i
$c_i \leftarrow Gen(1^$
Learning
Fixed-Time = t_{ft}
$(m_b) \leftarrow (m_0, m_1)$
$c^* \leftarrow Enc(pk, m_b)$
m_0, m_1
c^*, t_{ft}
$(m_0) \leftarrow \mathcal{M}$
$(m_1) \leftarrow \mathcal{M}$
$c^* = m_0$ or m
time = t_i
$m_i \leftarrow Dec(sk, c_i)$
c_i
m_i, t_i
$c_i \leftarrow Gen(1^$
Learning
Gen: Generator
Dec: Decryption Function
Enc: Encryption Function
$\mathcal{M}$: Plaintext Space

https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization/evaluation-criteria/security-(evaluation-criteria)

PQC SECURITY CATEGORIES (5-Level)

NIST will base its classification on the range of security strengths offered by the existing NIST standards in symmetric cryptography, which NIST expects to offer significant resistance to quantum cryptanalysis. In particular, NIST will define a separate category for each of the following security requirements (listed in order of increasing strength):

1.Any attack that breaks the relevant security definition must require computational resources comparable to or greater than those required for key search on a block cipher with a 128-bit key (e.g. AES128)

2.Any attack that breaks the relevant security definition must require computational resources comparable to or greater than those required for collision search on a 256-bit hash function (e.g. SHA256/ SHA3-256)

3.Any attack that breaks the relevant security definition must require computational resources comparable to or greater than those required for key search on a block cipher with a 192-bit key (e.g. AES192)

4.Any attack that breaks the relevant security definition must require computational resources comparable to or greater than those required for collision search on a 384-bit hash function (e.g. SHA384/ SHA3-384)

5.Any attack that breaks the relevant security definition must require computational resources comparable to or greater than those required for key search on a block cipher with a 256-bit key (e.g. AES 256)

Here, computational resources may be measured using a variety of different metrics (e.g., number of classical elementary operations, quantum circuit size, etc.). In order for a cryptosystem to satisfy one of the above security requirements, any attack must require computational resources comparable to or greater than the stated threshold, with respect to *all* metrics that NIST deems to be potentially relevant to practical security.

PQC

SÍNTESIS

Comenzar a pensar en PQC ya mismo…

- **Puede tomar 5 a 10 años actualizar la infraestructura tecnológica**
- **Aquí hay un sitio para enterarse en qué se ocupa la NIST acerca de PQC:**
  https://csrc.nist.gov/Projects/Post-Quantum-Cryptography
- **INVESTIGAR SOLUCIONES NACIONALES !!!**

desarrollos de PQC nacionales

•"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)