Post-Quantum Cryptography Using Hyper-Complex Numbers

Jorge Alejandro Kamlofsky[1] – Juan Pedro Hecht[2]

[1] CAETI - Universidad Abierta Interamericana.
Av. Montes de Oca 725 – Buenos Aires – Argentina.
Jorge.Kamlofsky@uai.edu.ar

[2] Universidad de Buenos Aires, Facultades de Ciencias Económicas, Ciencias Exactas y Naturales e Ingeniería. Maestría en Seguridad Informática, Buenos Aires, Argentina.
phecht@dc.uba.ar

Abstract. Encrypted communications are performed using symmetric ciphers, which require asymmetric cryptography for safe initiation. Asymmetric cryptography was seriously weakened after the presentation of Shor's algorithm (1997) and others for quantum computers. New algorithms are generalized as post quantum cryptography. Asymmetric cryptography based on non-commutative algebra is a growing trend arising as a solid choice that strengthens these protocols. Hyper-complex numbers generated by the Cayley-Dickson construction forms non-commutative algebras. This paper focus on the use of these numbers in post-quantum cryptography.

Keywords: octonion's cipher, quaternion's cipher, non-commutative cryptography, post-quantum cryptography, PCQ with hyper-complex numbers.

1 Introducción

1.1 Trabajos Relacionados

La criptografía se refiere a la ciencia o arte de diseñar criptosistemas. Su principal propósito es la protección de los intereses de las partes de una comunicación. Un criptosistema es un dispositivo diseñado para brindar tal protección. Se encripta la información de manera que solo pueda ser utilizada por quien esté autorizado [1]. Se distinguen dos instancias: el intercambio seguro de claves, y el encriptado y desencriptado del mensaje [2]. La criptografía puede dividirse, en dos ramas: simétrica, que encripta y desencripta los mensajes con una única clave compartida y asimétrica, que por un lado logra el intercambio seguro de claves y por el otro el cifrado de mensajes usando una clave pública y otra privada, hoy día con herramientas de la teoría de números.

Whitfield Diffie y Martin Hellman fueron los pioneros de la criptografía asimétrica: en 1976 presentaron el revolucionario concepto de criptografía de clave pública [3] cuya seguridad radica en el problema de la intratabilidad del logaritmo discreto [4] (*DLP: Discrete Logarithm Problem*). Sin embargo, por facilidad de implementación práctica, RSA [5] es hoy el esquema criptográfico de clave pública más usado. Su seguridad radica en el problema de la intratabilidad de la factorización de grandes números enteros *(IFP: Integer Factorization Problem)*. Es responsable en gran parte, de la seguridad en Internet, en las transacciones bancarias electrónicas o en la firma digital de correos electrónicos [6], entre otros.

En 1997 Peter Shor presentó un algoritmo que reduce drásticamente la complejidad computacional del problema IFP mediante una computadora cuántica [7]. Los trabajos de Kitaev [8] y Proos-Zalka [9] presentaron ataques eficaces a los problemas DLP y DLP para curvas elípticas también mediante computadora cuántica. A pesar que este dispositivo aún no se había inventado, la sola existencia de estos algoritmos, debilitó notoriamente a esta rama de la criptografía.

Desde inicios de este siglo ha crecido el interés por el desarrollo de criptosistemas asimétricos alternativos que sean resistentes a ataques de complejidad sub-exponencial y ataques a través de computadora cuántica [10 – 12]. A estos esquemas se los denomina colectivamente como criptografía post-cuántica (PQC: de sus siglas en inglés) [13]. Se han desarrollado diversas líneas de investigación PQC, conocidas hoy día como criptografía basada en polinomios multicuadráticos, en hashings, en retículos y en códigos [10, 14 - 16]. Sin desmedro de esas corrientes de estudio, se han buscado soluciones vinculadas con estructuras algebraicas no conmutativas y no asociativas [17]. Nuestros estudios se ubican en esta última corriente.

En general se usan estructuras algebraicas en las que el producto no cumple la propiedad conmutativa. Gracias a su naturaleza algebraica, a esta línea se la denomina criptografía no conmutativa [18]. No se conocen ataques concretos a esta línea que hayan logrado resultados exitosos. Dentro de esta línea, en [19] se presentó un esquema de distribución de claves Diffie-Hellman basado en un anillo de polinomios matriciales, inspirado en [20].

Dentro de esta clasificación, un subconjunto de elementos algebraicos es el conjunto de los números hipercomplejos creados a partir de la construcción de Cayley-Dickson: cuaterniones [21], octoniones [22], y otros. Dicha construcción [23] tiene la peculiaridad que en cada álgebra generada, se pierde una propiedad. A partir del álgebra de cuaterniones, el producto no es conmutativo. Criptosistemas no conmutativos con números hipercomplejos se presentaron en [24 - 26].

Como este proceso permite formar infinidad de álgebras no conmutativas, es de suponer que podrían desarrollarse infinidad de criptosistemas no conmutativos. Sin embargo, propiedades que se pierden en instancias de esta construcción hacen que ciertas álgebras carezcan de interés criptográfico. En este trabajo, se presenta un enfoque acerca del uso de números hipercomplejos en PQC.

1.2 Motivación y Alcance

Pareciera ser que la criptografía no conmutativa usando números hipercomplejos obtenidos a partir de la construcción de Cayley-Dickson no tuviera límite. Sin embargo, como a partir de elementos de dimensión 16 (sediniones) las álgebras generadas presentan divisores de cero, su interés criptográfico quedaría así acotado. Este trabajo muestra virtudes y límites en el uso de números hipercomplejos en PCQ.

1.3 Objetivo del Trabajo

La finalidad de este trabajo es presentar un enfoque que muestre las ventajas del uso de números hipercomplejos en criptografía no conmutativa pero a su vez pretende acotar su uso al armado de esquemas criptográficos con cuaterniones y octoniones.

1.4 Relevancia del tema

En los últimos lustros se han realizado desarrollos en línea con PQC. En 2016 la NIST declaró a PQC como un tema de interés, y llamó a presentación de propuestas para la implementación de algoritmia PCQ eficiente [27].

1.5 Estructura del Trabajo

En la Sección 2 se presenta el marco teórico. En la Sección 3 se presenta el enfoque propuesto con datos experimentales. La Sección 4 contiene las conclusiones.

2 Marco Teórico

2.1 La Criptografía y la Seguridad de las Comunicaciones

Nociones Básicas de la Criptografía Simétrica. A partir del inicio del cifrador, el mensaje se transforma en el punto de emisión mediante operaciones matemáticas de manera que sea imposible de interpretarlo mientras viaja en el canal inseguro, o bien su costo en tiempo y/o recursos sean tan altos que su descubrimiento carezca de sentido. Se usan algoritmos criptográficos muy robustos que permiten que la información se encripte bit a bit o en grupos de n-bits permitiendo que puedan cifrarse comunicaciones en tiempo real [4], sin que la encripción demore la transmisión del mensaje. Usan la misma clave para el cifrado y descifrado. Pueden iniciarse con claves de 128 bits, aunque recientes recomendaciones [28] imponen una longitud de claves para cifradores simétricos de 192 y 256 bits (AES: advanced encryption standard NIST).

Nociones Básicas de Criptografía Asimétrica. Usa elementos públicos que se comparten, y elementos privados que se mantienen en secreto. Tradicionalmente usan propiedades y operaciones de aritmética modular en estructuras algebraicas de campos de números enteros. Así se brindó soluciones al problema de presentar en forma segura claves para su uso en cifradores simétricos: mientras que mediante RSA [5] y ElGamal [29] se pueda enviar una clave simétrica cifrada a otro usuario que descifra usando su clave pública, con Diffie-Hellman [3] ambas partes pueden generar la misma clave intercambiando elementos.

Amenaza a la Criptografía: El Algoritmo de Shor y la Computación Cuántica. En 1997 Peter Shor presentó un algoritmo para computación cuántica basado en la transformada rápida de Fourier que logra resolver en tiempo polinómico el problema IFP [7]. Es decir, permite reducir drásticamente la complejidad del problema (considerado de clase NP) a niveles atacables [30]. Una computadora cuántica usa qubits en lugar de bit. Un qubit posee los estados clásicos 0 o 1 en superposición, realizando cómputos en forma paralela sobre ambos y que finalmente se resuelven en bits clásicos por decoherencia. Por ello, se puede realizar una cantidad exponencial de operaciones en paralelo en relación exponencial con la cantidad de qubits del computador cuántico. La computación cuántica prácticamente arrasa con todo lo conocido en la criptología actual: con ello desaparecen de escena prácticamente todos los criptosistemas de clave pública actualmente en uso.

Criptografía Post-Cuántica Basada en Álgebra no Conmutativa. En este trabajo, se utilizan estructuras de anillos de polinomios de matrices cuadradas o de cuaterniones, entre otros, con elementos finitos, por lo tanto, su seguridad radica en la complejidad del tratamiento del problema DLP. Nuestros esquemas se basan en la dificultad de resolver el problema SDP (*Symmetric Descomposition Problem*) [19] en un anillo no conmutativo de polinomios matriciales. Desde el punto de vista criptográfico, solo se necesita estar seguro que no exista fórmula que permita reducir la complejidad del problema DLP (incluso con computadora cuántica). Y esto está garantizado ya que en los anillos no conmutativos no existe forma conocida de relacionar el determinante de una matriz o bien sus autovalores con la potencia de la matriz [31], parte de la clave privada, independientemente de la cantidad de qubits que pudiera tener una computadora cuántica que ejecute el ataque.

2.2 Los Numeros Hipercomplejos

Son una extensión de los números complejos construidos mediante herramientas del álgebra abstracta, tales como terniones, cuaterniones, tesarines, octoniones, sedeniones, y demás. Tienen más de una componente compleja. Muchos conforman álgebras que carecen de interés dentro de nuestro análisis [32].

La Construcción de Cayley-Dickson. La construcción de Cayley-Dickson produce una secuencia de álgebras sobre el cuerpo de los números reales. Cada álgebra producida posee el doble de la dimensión de la anterior. En cada etapa, al generarse una nueva álgebra, esta pierde una propiedad algebraica específica [22].

Proceso General. Como lo notó Hamilton [21], el complejo $a + bi$ puede entendérselo como el par de números reales (a , b). La suma se hace componente a componente y el producto con otro complejo (c , d) se hace de la siguiente forma:

$$(a , b).(c , d) = (ac - db , ad + cb)$$

También puede definirse el conjugado de un complejo como: $(a , b)^* = (a , - b)$. De esta forma ya se han obtenido los números complejos, a partir de los reales. Los cuaterniones pueden definirse de forma análoga. Es decir, pueden ser pensados como un par de números complejos y obtener suma, producto, conjugación y norma. Repitiéndose el proceso, se pueden hallar las álgebras de dimensión superior.

Propiedades Perdidas en el Proceso. Al aplicarse el proceso de Cayley-Dickson al cuerpo de los reales y obtenerse el cuerpo de los complejos, se pierde la relación de orden. Su aplicación sobre el cuerpo de los complejos forma el álgebra de cuaterniones: les hace perder la propiedad conmutativa. Los cuaterniones forman entonces, estructura de anillo de división. Aplicando el proceso sobre el anillo de cuaterniones se genera el álgebra de octoniones: se pierde la propiedad asociativa. Los octoniones, forman un álgebra de división normada. La conformación del álgebra de Sediniones (16 componentes) le quita la propiedad de ser álgebra de división, lo que se hereda a las posteriores álgebras superiores generadas tras aplicaciones sucesivas del proceso, haciéndolas poco interesantes para su uso en PQC.

Finalmente, el uso de números hipercomplejos que forman álgebras no conmutativas, para su uso en PQC se limita entonces, a cuaterniones y octoniones.

Anillo de Cuaterniones. Un anillo (A ; + ; .) es una estructura algebraica (un conjunto A con las operaciones suma y producto) donde (A ; +) forman estructura de grupo, y (A ; .) de semigrupo. Y el producto es distributivo (por los dos lados) respecto de la suma. Un anillo es no conmutativo si no se verifica la propiedad conmutativa entre todos los elementos de A para la operación producto.

El primer anillo de división (cuyos elementos no nulos son inversibles) no conmutativo fue el anillo de los cuaterniones [21].

Definición: Cuaternión. Sea (H ; + ; .) un anillo conmutativo con unidad. Un cuaternión q con coeficientes en H es un número hipercomplejo de la forma: $q = a + b.i + c.j + d.k$, donde $a, b, c, d \in R$; i, j, k son unidades imaginarias que verifican que: $i^2 = j^2 = k^2 = - i.j.k = - 1$, y además: $i.j = -j.i = k$; $j.k = -k.j = i$; $i.k = -k.i = j$.

Operaciones Básicas: suma, resta y producto de un escalar por un cuaternión se realiza de la misma forma que con cualquier vector de 4 dimensiones. Para el producto entre cuaterniones debe tenerse en cuenta el producto entre unidades imaginarias. Puede encontrarse información más detallada en [24].

Álgebra de Octoniones. Los octoniones forman un álgebra de división normada. Fueron descubiertos por John T. Graves en 1843, e independientemente por Arthur

Cayley. Se usaron recientemente en Física, para dar sustento a la teoría de cuerdas [33]. El conjunto de Octoniones no nulos con la operación producto forman una estructura de bucle (loop) de Moufang no asociativo [34].

*Definición: Octonión. E*s una expresión de la forma $o = \alpha_0. + \alpha_1.e_1 + \alpha_2.e_2 + \alpha_3.e_3 + \alpha_4.e_4 + \alpha_5.e_5 + \alpha_6.e_6 + \alpha_7.e_7$ donde α_i son números reales y e_i unidades imaginarias. Puede ser representado como un vector de 8 componentes.

Operaciones Básicas: Suma, Resta y Producto de un Escalar por un Octonión se realiza de la misma forma que con cualquier vector de 8 dimensiones. Para el producto entre octoniones debe tenerse en cuenta el producto entre unidades imaginarias [22]. Puede encontrarse información más detallada en [26]. El producto de octoniones es cerrado, tiene elemento neutro, pero no cumple las propiedades conmutativa ni asociativa.

3 Implementaciones Criptográficas con Números Hipercomplejos

Se limitan al uso de cuaterniones y octoniones. En esta sección se hace referencia a esquemas de intercambio de claves Diffie-Hellman: una vez logrado esto, es fácil derivar a otros esquemas asimétricos [20]. En [24] se presentó un esquema Diffie Hellman inspirado en [19], implementado con polinomios de cuaterniones: llamado DHCQ. Junto con la mejora propuesta en [25] se logró reducir notablemente los tiempos de proceso. En [26] se presenta un esquema similar implementado con octoniones: llamado DHECO. Ambos sistemas se los denomina compactos ya que son aptos para procesadores de pequeño porte gracias a no requerir de librerías de precisión extendida, y se presentan versiones para procesadores de 8 bits, 16 bits y 32 bits. DHECO funciona solo con operaciones suma-producto, lo que permite que sea implementado en procesadores muy elementales. Promete ser bastante más robusto. Pero sus tiempos de procesamiento son mayores. Ambos esquemas son inmunes a ataques subexponenciales y de computadora cuántica.

En esta sección se presentan los conceptos básicos de ambos esquemas con datos experimentales. Más detalles pueden obtenerse de los trabajos originales [24 - 26].

3.1 DHCQ: Esquemas de Intercambio de Claves Usando Cuaterniones

El Protocolo. Alice elige dos cuaterniones aleatorios A y B, con elementos de $Z_{2^{k*8}}$ (con k = 1, k = 2, k = 4) y los normaliza: q_A y q_B. Elige como clave privada dos números enteros aleatorios m y n en Z_{16}, y un polinomio entero $f(x)$ con coeficientes y exponentes en Z_{16} tal que $f(q_A) \neq 0$ y envía a Bob por el canal inseguro los elementos q_A y q_B. Bob elige como clave privada dos números enteros aleatorios r y s en Z_{16}, y un polinomio entero $h(x)$ con coeficientes y exponentes en Z_{16} tal que $h(q_A) \neq 0$. Ambos realizan las normalizaciones de $f(q_A)$ y $h(q_A)$: $f'(q_A)$ y $h'(q_A)$. Alice calcula su token: $r_A = f'(q_A)^m.q_B.f'(q_A)^n$. Bob calcula el suyo: $r_B = h'(q_A)^r.q_B.h'(q_A)^s$; y se los intercambian para el cálculo de las claves: $k_A = f'(q_A)^m.r_B.f'(q_A)^n$ (Alice), $k_B = h'(q_A)^r.r_A.h'(q_A)^s$ (Bob). Se modularizan: $K_A = k_A \,.\, 2^{k*16}\ (mod\ 2^{k*16})$, $K_B = k_B \,.\, 2^{k*16}\ (mod\ 2^{k*16})$ con $K_A = K_B$.

3.2 DHECO: Esquemas de Intercambio de Claves Usando Octoniones

Resumen del Protocolo. Alice elige dos octoniones aleatorios o_A y o_B, con elementos de $Z_{k*8bits}$ (con k = 1, 2 o 4). Elige como clave privada dos números enteros aleatorios m y n en Z_{16} y un polinomio entero $f(x)$ con coeficientes y exponentes en Z_{16} tal que $f(o_A) \neq 0$. y los envía a Bob por el canal inseguro. Bob elige como clave privada dos números enteros r y s en Z_{16}, y un polinomio entero $h(x)$ con coeficientes y exponentes en Z_{16} tal que $h(o_A) \neq 0$. Alice calcula su token: $r_A = (f(o_A)^m.o_A).f(o_A)^n$. Bob calcula el suyo: $r_B = (h(o_A)^r.o_B).h(o_A)^s$ y se los intercambian para el cálculo de las claves: $K_A = (f(o_A)^m.r_B).f(o_A)^n$ (Alice), $K_B = (h(o_A)^r.r_A).h(o_A)^s$ (Bob). Luego: $K_A = K_B$.

La figura 1 muestra un esquema del protocolo propuesto.

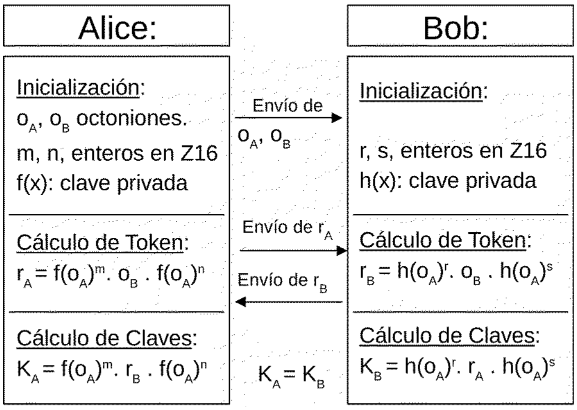

Fig. 1: Esquema del protocolo propuesto.

3.3 Seguridad Adicional.

Si bien el uso tanto de cuaterniones como de octoniones garantiza la ausencia de divisores de cero, el álgebra en el anillo de enteros (en las componentes de los cuaterniones o de los octoniones) posee divisores de cero si el módulo no es primo, presentando efectos no deseados. Para evitar este inconveniente, se trabaja con módulo: el mayor primo menor a K*8bits. Esto es: si k = 1, las componentes del cuaternión u octonión son elementos en $Z^*_{251.}$ Si k = 2 sus componentes son elementos en Z^*_{65521}. Y si k = 4 sus componentes son elementos en $Z^*_{4294967279}$.

La seguridad de los protocolos presentados en [24 - 26] se ha fortificado: En lugar de que ALICE publique los enteros m y n, aquí se los usa como parte de su clave secreta. BOB por su parte elige sus propios enteros secretos r y s en lugar de repetir los m, n que publicó ALICE. Ello dificulta aún más el problema SDP.

3.4 Datos Experimentales

Equipamiento Usado. El computador usado tiene un procesador Intel® Core™ i3-2328M CPU @ 2.20GHz × 4 y 3,7 GiB RAM. Sistema operativo Kali GNU/Linux 64-bit, con un núcleo Debian. Los algoritmos fueron programados en Python 2.7.10.

Versiones Propuestas. Cada valor de k genera una versión para cada criptosistema: 8, 16 y 32 bits. Se presentan en 8 bits: DHCQ8 y DHECO8. En 16 bits: DHCQ16 y DHECO16. En 32 bits: DHCQ32 y DHECO32.

Resultados Experimentales. Se presenta una comparación de los tiempos de ejecución para la obtención de 1000 claves de 256 bits entre los diferentes esquemas y versiones. La tabla 1 muestra los resultados experimentales.

Tabla 1. Tiempos de ejecución para la obtención de 1.000 claves de 256 bits.

	CPU Time (s)								
Nº Test	DHCM8 8-bits	DHCM16 16-bits	DHCM32 32-bits	DHCQ8 8-bits	DHCQ16 16-bits	DHCQ32 32-bits	DHECO8 8-bits	DHECO16 16-bits	DHECO32 32-bits
1	4,9232	2,6201	4,9177	3,7838	1,9273	1,0624	10,8278	5,4771	4,9928
2	4,8215	2,6124	5,0230	3,8360	1,7862	0,9280	10,8237	5,4119	5,4673
3	4,9672	2,5244	4,9549	3,5639	1,8374	0,8861	11,0357	5,5073	5,0466
4	4,9166	2,6128	4,9277	3,6088	1,8602	0,9133	11,0351	5,4587	4,9441
5	4,8174	2,6365	5,0176	3,7249	1,8298	0,9343	11,2985	5,5615	4,9406
6	4,9174	2,6104	4,9433	3,6658	1,8519	0,9102	10,8646	5,5769	5,0594
7	4,9207	2,5530	5,2199	3,6511	1,7609	1,0421	11,1051	5,5226	4,9823
8	4,8164	2,6122	4,9217	3,7963	1,8615	0,9048	11,0446	5,4649	5,0472
9	4,8456	2,6124	5,0184	3,6306	1,8013	0,9627	11,1739	5,4660	4,8783
10	4,8163	2,5378	5,0295	3,6095	1,8660	0,9449	11,4447	6,2083	4,9739
Promedio	4,8762	2,5932	4,9974	3,6871	1,8383	0,9489	11,0654	5,5655	5,0333

3.5 Ventajas de los Esquemas Propuestos

Mayor Velocidad del Esquema DHCQ. En todas sus versiones presenta menores tiempos de ejecución en comparación con implementaciones con matrices [19].

Mayor Robustez del Esquema DHECO. Los esquemas basados en álgebra no asociativa son aún más resistentes que los cripto-sistemas no conmutativos. Por tratarse de un sistema algebraico no conmutativo y no asociativo, los octoniones no admiten representación matricial. Las potencias se deben calcular en forma exclusivamente recursiva, impidiendo la localización de potenciales generadores u órdenes multiplicativos por medio del algoritmo de Shor, base del ataque cuántico que requiere que la estructura sea un campo, es decir producto asociativo.

Esquemas Aptos para Procesadores de Pequeño Porte. No requerir librerías de precisión extendida los hace apto para procesadores pequeños. En especial, DHECO solo usa operaciones suma-producto, haciéndolo apto para procesadores elementales.

Inmunidad Frente a Ataques de Complejidad Sub-Exponencial o de Computadora Cuántica: No se conocen aún ataques de estos tipos a estructuras algebraicas no conmutativas que hayan sido efectivos y que debiliten su seguridad.

4 Conclusiones

La construcción de Cayley-Dickson a partir de los números complejos genera álgebras de números hipercomplejos que verifican el no cumplimiento de la propiedad conmutativa, lo cual es de interés en PCQ. Se concluye que solo las álgebras de cuaterniones y octoniones poseen interés criptográfico.

Las soluciones presentadas en [24 - 26] y aquí mencionadas, son esquemas de intercambio de claves Diffie Hellman implementados con cuaterniones y octoniones. Sin embargo, en general, lograr otros esquemas asimétricos una vez logrado uno de ellos, no suele presentar grandes dificultades.

Referencias

1. Barreno, Marco A.: The Future of Cryptography Under Quantum Computers. Dartmouth College Computer Science Technical Reports (2002).
2. Marrero Travieso, Yran: La Criptografía como elemento de la seguridad informática. ACIMED 11.6 (2003).
3. Diffie W., Hellman M.E: New directions in cryptography. IEEE Transactions on information theory, 22, 644-654, (1976).
4. Menezes, Alfred J., Paul C. Van Oorschot, and Scott A. Vanstone: Handbook of applied cryptography. CRC press (1996).
5. Rivest, Ronald L., Adi Shamir, and Len Adleman: A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM 21.2, 120-126. (1978)
6. Navarro Robles, Pedro Ramón: Intercambio de claves sobre anillos no conmutativos: End (Zp X Zp2) y extensiones. (2014).
7. Shor P.: Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, SIAM J. Comput., 5, 1484-1509 (1997).
8. Kitaev A.: Quantum measurements and the abelian stabilizer problem, Preprint arXiv/quant-ph., 9511026 (1995).
9. Proos J., Zalka C.: Shor's discrete logarithm quantum algorithm for elliptic curves. Quantum information and computation, 3, 317-344 (2003).

10. Bernstein, Daniel J., Johannes Buchmann, and Erik Dahmen.: Post-Quantum Cryptography. (2007).
11. Magliveras S.S., Stinson D.R., van Trung T.: New approaches to designing public key cryptosystems using one-way functions and trapdoors in finite groups. Technical Report CORR, 2000-2049 (2000).
12. Shpilrain V., Zapata G.: Combinatorial group theory and public-key cryptography, Preprint arXiv/math.gr, 0410068 (2004).
13. Barreto, P. et al.: Introdução à criptografia pós-quântica, Minicursos do XIII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais, SBSeg, (2013).
14. Kaya K. Open Problems in Mathematics & Computational Science, Springer Verlag, (2014).
15. Chen L. et al, NISTIR 8105, Report on Post-Quantum Cryptography, NIST. [En Linea], (2006). Disponible en: <http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf> . Fecha de consulta: 20/04/2017.
16. Moody, D.: Update on the NIST Post-Quantum Cryptography Project, 2016 http://csrc.nist.gov/groups/SMA/ispab/ (consulted April 20, 2017).
17. Kalka, A.: Non-associative public-key cryptography. arXiv:1210.8270, (2012).
18. Gerritzen L. et al (Editors): Algebraic Methods in Cryptography, Contemporary Mathematics, AMS, Vol. 418, (2006)
19. Hecht J.: Un modelo compacto de criptografía asimétrica empleando anillos no conmutativos. V Congreso Iberoamericano de Seguridad Informática, Montevideo (2009).
20. Cao Z., Xiaolei D., Wang L. New public-key cryptosystems using polynomials over non-commutative rings. Preprint arXiv/cr, eprint.iacr.org/2007/009.pdf (2007).
21. Hamilton, W. R. Lectures on Quaternions: Containing a Systematic Statement of a New Mathematical Method. Hodges and Smith, (1853).
22. Baez, J.: The Octonions. Bulletin of the American Mathematical Society 39.2 (2002)
23. Korniłowicz, Artur.:: Cayley-Dickson Construction. Formalized Mathematics 20.4 (2012)
24. Kamlofsky J., Hecht J., Abdel Masih S., and Hidalgo Izzi, O.: A Diffie-Hellman Compact Model Over Non-Commutative Rings Using Quaternions. VIII Congreso Iberoamericano de Seguridad Informática, Quito (2015).
25. Kamlofsky, J.: Improving a Compact Cipher Based on Non Commutative Rings of Quaternion. En XXII Congreso Argentino de Ciencias de la Computación CACIC, (2016).
26. Kamlofsky, J., Hecht, J. y Abdel Masih, S.: Post-Quantum Cryptography: An Elementary and Compact Key Exchange Scheme Based on Octonions. Presentado en: IX Congreso Iberoamericano de Seguridad Informática CIBSI. (2017).
27. National Institute of Standards and Technology, Information Technology Laboratory – Computer Security Division. “Post-Quantum Crypto Proyect”. [En línea], (2016) Disponible en: <http: // csrc.nist.gov / groups / ST / post-quantum-crypto/>. Fecha de consulta: 11/06/2017.
28. Barker E., Roginsky, A.: Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths. NIST Special Publication 800-131A (2015).
29. EGamal, Taher. A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms. En Advances in cryptology. Springer Berlin Heidelberg, pp. 10–18 (1984).
30. Hecht, JP.: Fundamentos de Computación Cuántica. Editorial Académica Española, (2005).
31. Eftekhari, M.: A Diffie–Hellman key exchange protocol using matrices over noncommutative rings. Groups-Complexity-Cryptology, 4(1), pp. 167–176 (2012)
32. Kenneth O. May,: The impossibility of a division algebra of vectors in three dimensional space; American Mathematical Monthly, Vol 73, No. 3 (1966) 289-291.
33. Baez, J, et Huerta, J.: Des octonions pour la théorie des cordes. Pour la science 406 (2011).
34. Belousov, V. D.: "Moufang loops", Hazewinkel, Michiel, Encyclopedia of Mathematics, Springer (2001).