Post-Quantum Cryptography: An Elementary and Compact Key Exchange Scheme Based on Octonions

Jorge Kamlofsky[1] –Pedro Hecht[2] – Samira Abdel Masih[3]

[1,3] 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*— To start encrypted communications between two entities using symmetric cryptography, an asymmetric cryptography protocol like Diffie-Hellman is normally used to generate the required session keys. Most protocols are based on modular operations over integer's rings. Many are vulnerable to sub-exponential attacks or by using a quantum computer. Cryptography based on non-commutative and non-associative structures are a growing trend as a solid option to reinforce these protocols. In particular, Hecht (2009) has presented a key exchange model based on the Diffie-Hellman protocol using matrices of order four with elements in Z_{256}, that provides 128-bits keys also to devices with low computing power. Kamlofsky et al (2015) presented a quickest model using quaternions. Quaternions are four-component's vectors that form a non-commutative skew field. Octonions can be formed from quaternions. They form a non-commutative and non-associative ring structure. This paper presents an elementary and compact key exchange scheme using octonions.

***Index Terms* — Asymmetric cryptography, Post-quantum cryptography, Non-commutative cryptography, Non-associative cryptography, Hyper complex numbers**

I. Introducción

A. Trabajos Relacionados

Criptografía es una rama de la Matemática que trata el problema de enviar información en forma confidencial a través de un medio inseguro: se cifra la información de manera que, aún cuando se encuentre disponible para cualquiera, no pueda ser utilizada, a menos que alguien autorizado la descifre. En una comunicación cifrada, entonces, pueden presentarse dos instancias diferentes: el intercambio seguro de claves y luego, con ello, el cifrado y descifrado del mensaje [1]. La Criptografía, entonces, se divide en dos grandes ramas: de clave privada o simétrica, que cifra y descifra los mensajes y de clave pública o asimétrica, que logra el intercambio seguro de claves.

Diffie y Hellman fueron los pioneros de la criptografía asimétrica: en 1976, en [2] presentaron el revolucionario concepto de criptografía de clave pública cuya seguridad radica en el problema de la intratabilidad del logaritmo discreto [3] (*DLP: Discrete Logarithm Problem*). El esquema criptográfico de clave pública más usado hoy es RSA [4]: su seguridad radica en el problema de la intratabilidad de la factorización de grandes números enteros *(IFP: Integer Factorization Problem)*.

En 1993 Peter Shor presentó un algoritmo que reduce la complejidad computacional del problema IFP mediante una computadora cuántica [5]. A pesar que este dispositivo aún no se había inventado, sólo la existencia del algoritmo, logró debilitar a esta rama de la criptografía. Hoy su existencia es un hecho: la empresa D-Wave Systems ya vendió computadoras cuánticas a Lockheed Martin, al laboratorio Los Alamos, a Google y a la NASA, entre otros [6]. Además, IBM por su lado, ofrece servicios en la nube con su computadora cuántica [7].

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 vía computadora cuántica [8 – 9]. La mayoría de estos esquemas son denominados colectivamente como criptografía post-cuántica [10]. O bien, por su naturaleza algebraica, se los denomina criptografía no conmutativa [11]. Sobre esta línea, no se conocen ataques que hayan logrado resultados concretos. Dentro de esta línea, en [12] se presentó un esquema de distribución de claves Diffie-Hellman basado en un anillo de polinomios matriciales. Al sistema se lo denominó compacto debido a que no se requieren librerías de precisión extendida, lo que hace posible su uso en procesadores de menor porte. En [13] se implementó dicho esquema en un anillo de polinomios de cuaterniones, lo cual permitió la obtención de claves de la misma longitud (128 bits) con una mejora notoria en los tiempos de ejecución. En [14] se presentó una mejora basada en el cambio del conjunto numérico de módulo 8 bits a módulo 16 y 32 bits con resultados remarcables.

La criptografía no conmutativa y no asociativa se presenta como una opción más robusta [15, 17]. Los octoniones conforman estructura de anillo no conmutativo no asociativo.

En este trabajo, se presenta un esquema de intercambio de claves basado en octoniones. Se lo llama ‘compacto’ debido a que para su funcionamiento no requiere de librerías de precisión extendida. Más aún, el protocolo presentado solo realiza operaciones suma-producto, lo que permite que sea aplicable a procesadores muy simples, de bajo porte. Por esto se lo llama ‘elemental’.

B. Motivación y Alcance:

Las matrices y los cuaterniones conforman estructuras de anillos donde no se cumple la propiedad conmutativa. Los octoniones, además, no cumplen la propiedad asociativa. Sedeniones y otros números hipercomplejos de álgebras de mayor dimensión tampoco cumplen la propiedad conmutativa ni asociativa, pero carecen de interés criptográfico ya que posee divisores de cero.

En [12-14] se presentaron esquemas de intercambio de claves Diffie-Hellman compactos basados en matrices y cuaterniones. Sin embargo, no hay implementación similar realizada con octoniones.

C. Objetivo de este Trabajo:

Presentar un esquema de intercambio de claves Diffie Hellman Compacto usando álgebra no asociativa mediante octoniones.

D. Relevancia del Tema:

La implementación del algoritmo de Shor en una computadora cuántica es una realidad del futuro cercano. En caso de concretarse, la criptografía asimétrica clásica basada en campos numéricos conmutativos se encuentra bajo riesgo de desaparición [30]. Los nuevos desarrollos en criptografía post-cuántica, como el que aquí se presenta, permiten resolver esta debilidad.

E. Estructura del Trabajo:

En la Sección 2 se presenta el marco teórico. En la Sección 3 se presenta al protocolo propuesto. La sección 4 contiene resultados experimentales. En la Sección 5 se presentan las conclusiones y luego los trabajos futuros.

II. Marco Teórico

A. La Importancia de la Criptografía en la Seguridad de las Comunicaciones:

Nociones Básicas de Criptografía Simétrica. La Criptografía se ocupa de asegurar la integridad y confidencialidad en las comunicaciones a través de un canal inseguro. Para ello, 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 altamente robustos que permiten además que la información se encripte bit a bit (cifradores de flujo) o en grupos de n-bits (cifradores de bloque) permitiendo que puedan cifrarse comunicaciones en tiempo real [3]. Estos sistemas usan la misma clave para el cifrado y descifrado del mensaje. A estos cifradores se los clasifica como Criptografía Simétrica. Criptosistemas simétricos seguros como AES y 3DES, pueden iniciarse con claves de 128/192/256 bits o 112/168 bits respectivamente. Las recomendaciones recientes de la NIST en la SP 800-131A Rev. 1 [18] para cifradores simétricos es usar claves de 256 bits.

Nociones Básicas de Criptografía Asimétrica. La criptografía asimétrica o de clave pública, usa elementos públicos que se comparten, y elementos privados que se mantienen en secreto. Los sistemas más difundidos hoy día, usan propiedades y operaciones de aritmética modular en estructuras algebraicas de anillos de números enteros.

Ésta brindó, entre otras, soluciones al problema de presentar en forma segura claves para su uso en cifradores simétricos: con Diffie-Hellman [2] ambas partes pueden generar la misma clave simétrica intercambiando elementos y los algoritmos RSA [4] y ElGamal [19] permiten que se pueda enviar esa clave simétrica en forma cifrada a otro usuario usando la clave pública del receptor, si se emplea criptografía híbrida.

Amenaza a la Criptografía: El Algoritmo de Shor y la Computación Cuántica. En 1995 Peter Shor presentó un algoritmo para computación cuántica basado en la transformada rápida de Fourier (FFT) que logra resolver en tiempo polinómico el problema IFP [5]. Es decir, permite reducir drásticamente la complejidad del problema (considerado tentativamente de clase de complejidad temporal NP) a niveles atacables [20].

Una computadora cuántica usa qubits en lugar de bits. Un qubit posee la superposición de los estados clásicos 0 y 1. Por ello, se pueden realizar una cantidad exponencial de operaciones en paralelo cuya potencia crece en relación con la cantidad de qubits del computador cuántico.

En 2001 se implementó el algoritmo de Shor en la primera computadora cuántica. En caso de convertirse en realidad práctica, hecho que da por sentado la NIST para un futuro cercano [30], arrasa con la casi totalidad de los algoritmos en la criptografía actual. Los más afectados serían los criptosistemas de clave pública RSA, las variantes de campos numéricos y ciertas variantes de campos algebraicos (Curvas Elípticas) que emplean los algoritmos ElGamal y Diffie-Hellman [20].

B. Criptografía Post-Cuántica Basada en Anillos no Conmutativos y no Asociativos.

Se utilizan estructuras de anillos de matrices cuadradas, de cuaterniones u octoniones entre otros, conformados por números enteros, por lo tanto, su seguridad radica en la complejidad del tratamiento del problema DLP. Algunos esquemas como el presentado en [21] se basan en la dificultad de resolver el problema SDP (*Simple Descomposition Problem*) en un anillo no conmutativo de polinomios matriciales.

Desde el punto de vista criptográfico, sólo se necesita estar seguro de que no existe 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 de relacionar el determinante de una matriz o bien sus eigenvalores con la potencia de la matriz [22], parte de la clave privada, independientemente de la cantidad de qubits que pudiera tener una computadora cuántica

que ejecute el ataque. En [12] se muestran más consideraciones de la seguridad de estos esquemas.

Mientras que la seguridad de la mayoría de los protocolos de la criptografía que usan álgebra no conmutativa se basa en el problema del conjugado o sus derivados, la criptografía no conmutativa y no asociativa se presenta como una línea criptográfica más fuerte [15]. Kalta et al [16] han generalizado el ingenioso protocolo de intercambio de claves (KEP: de sus iniciales en inglés) Anshel-Anshel-Goldfeld para monoides [17] a un KEP para magmas, estableciendo la criptografía de clave pública no asociativa. Los octoniones conforman estructura de anillo no conmutativo no asociativo, y son un ejemplo de números hipercomplejos que conforman estructura de magma.

Aplicando la construcción de Cayley-Dickinson sobre octoniones puede obtenerse una secuencia de álgebras de dimensión 16, 32, 64 y más. Pero todas estas álgebras tienen divisores de cero. Por lo tanto, por el momento parecen de carecer de interés criptográfico [23].

C. Origen y Uso de los Octoniones:

Anillos no Conmutativos. Un anillo (A ; + ; .) es una estructura algebraica (un conjunto A no vacío con las operaciones suma y producto) donde (A ; +) forman estructura de grupo, y (A ; .) de semigrupo. Además, debe cumplir con la propiedad distributiva del producto respecto de la suma con elementos del anillo. Será no conmutativo si no se verifica la propiedad conmutativa del producto entre todos los elementos de A.

El primer anillo de división (cuyos elementos no nulos son invertibles) no conmutativo fue el anillo de los cuaterniones [23]. Otro ejemplo es el conjunto de matrices cuadradas de orden n con coeficientes en A (simbolizado por $M_n(A)$), es un anillo con respecto a las operaciones usuales de suma y producto de matrices. Si $n > 1$, entonces $M_n(A)$ no es conmutativo.

Es importante destacar que los únicos elementos del álgebra no conmutativa que conforman álgebras de división (y por ende no se generan divisores de cero), son los cuaterniones y los octoniones. Esto otorga mayor fortaleza a los criptosistemas que los usan.

Origen de los Octoniones: Fueron descubiertos por John T. Graves en 1843, e independientemente por Arthur Cayley, quien lo publicó por primera vez en 1845. Por esta razón son a veces llamados "Los números de Cayley".

Un octonion puede formarse a partir de un par de cuaterniones usando la construcción de Cayley-Dickson así como los cuaterniones pueden formarse a partir de un par de números complejos. Usando esto, a partir de un álgebra n-dimensional puede obtenerse una nueva álgebra de dimensión 2n. Pero cada una de estas nuevas álgebras pierde una propiedad: mientras el álgebra de complejos es conmutativa y asociativa, el álgebra de cuaterniones es asociativa, pero no conmutativa. El álgebra de octoniones pierde la propiedad asociativa [24].

Los Octoniones en la Física: Al principio, los octoniones no parecieron ofrecer aplicaciones a la Geometría ni a la Física, por lo que fueron castigados a un rincón. En 1925, Elie Cartan los utilizó para descubrir el fenómeno de la trialdad, que es la simetría existente entre vectores y espinores en dimensión 8. Más tarde, en 1936, su importancia en Física fue vislumbrada en un trabajo de Jordan, Von Neumann y Wigner sobre los fundamentos de la Mecánica Cuántica, aunque después no hubo resultados relevantes [25].

Según la teoría de cuerdas [26], en los niveles fundamentales, el universo exhibe una simetría entre materia y fuerzas de la naturaleza: cada partícula de materia tiene asociada una partícula que lleva una fuerza. A este concepto se lo denomina Super-simetría.

Si se tiene en cuenta el efecto del tiempo, se obtienen super-simetrías en 3, 4, 6 y 10 dimensiones. Y en la teoría de cuerdas para 10 dimensiones las partículas de fuerza y materia se expresan mediante octoniones [27].

D. Álgebra Básica de Octoniones:

Definición: Un octonion es una expresión de la forma $o = \alpha_0 + \sum_{i=1}^{i=7} \alpha_i \, . \, e_i$ donde $\alpha_i \in R, e_i$ son unidades imaginarias. Puede ser representado como un vector de 8 componentes.

Suma: Sean los octoniones $o_1 = (a_1 , b_1 , c_1 , d_1 , e_1 , f_1 , g_1 , h_1)$ y $o_2 = (a_2 , b_2 , c_2 , d_2 , e_2 , f_2 , g_2 , h_2)$. La suma de dos octoniones resulta en otro octonion que se obtiene realizando la suma componente a componente: $o = o_1 + o_2 = (a_1 + a_2 , b_1 + b_2 , c_1 + c_2 , d_1 + d_2 , e_1 + e_2 , f_1 + f_2 , g_1 + g_2 , h_1 + h_2)$.

La suma cumple las siguientes propiedades: Ley de composición interna, conmutativa, asociativa, existencia de simétrico y elemento neutro.

Producto: Las unidades imaginarias se multiplican según se indica en la Tabla 1.

El producto de octoniones es cerrado, tiene elemento neutro, pero no cumple las propiedades conmutativa ni asociativa. El conjunto de Octoniones no nulos con la operación '.' (producto) forman una estructura de bucle (*loop*) de Moufang no asociativo [28].

A los fines de detallar las operaciones con octoniones necesarias para la implementación del modelo propuesto, lo anteriormente descripto es suficiente. En [24] pueden obtenerse más detalles acerca de las operaciones con octoniones.

Tabla 1: Producto entre unidades imaginarias.

·	1	e_1	e_2	e_3	e_4	e_5	e_6	e_7
1	1	e_1	e_2	e_3	e_4	e_5	e_6	e_7
e_1	e_1	-1	e_4	e_7	$-e_2$	e_6	$-e_5$	$-e_3$
e_2	e_2	$-e_4$	-1	e_5	e_1	$-e_3$	e_7	$-e_6$
e_3	e_3	$-e_7$	$-e_5$	-1	e_6	e_2	$-e_4$	e_1
e_4	e_4	e_2	$-e_1$	$-e_6$	-1	e_7	e_3	$-e_5$
e_5	e_5	$-e_6$	e_3	$-e_2$	$-e_7$	-1	e_1	e_4
e_6	e_6	e_5	$-e_7$	e_4	$-e_3$	$-e_1$	-1	e_2
e_7	e_7	e_3	e_6	$-e_1$	e_5	$-e_4$	$-e_2$	-1

III. El Protocolo Propuesto

A. Algunos Sistemas Compactos de Intercambio de Claves Diffie-Hellman Basados en Álgebra No Conmutativa:

Esquema Diffie - Hellman Compacto con Matrices (DHCM). En [12] se presentó un sistema de intercambio de claves Diffie Hellman [2] sobre anillos de matrices de enteros con elementos en Z_{256}, que utiliza como clave privada un polinomio con coeficientes y exponentes en Z_{16}.

Un par de ventajas surgen de ello. Primero: no se requiere el uso de librerías de precisión extendida, por lo tanto, puede ser usado en procesadores de pequeño porte. De allí la calificación de compacto. La otra ventaja se relaciona con el hecho que las matrices conforman estructura de anillo no conmutativo. Gracias a ello, el esquema se presenta como inmune a ataques cuánticos y ataques de complejidad sub-exponencial.

La clave resultante es una matriz de orden 4 con elementos en Z_{256} conformando así una clave de 128 bits, adecuada para su uso en sistemas de cifrado simétrico tipo AES.

Esquema Diffie-Hellman Compacto con Cuaterniones (DHCQ). Diversas aplicaciones pueden implementarse con cuaterniones en lugar de matrices cuadradas, en menores tiempos de ejecución [29]. Ello inspiró el desarrollo del esquema propuesto en [13], que resultó en un ahorro de tiempo cercano al 50% bajo condiciones similares. El cálculo se realiza con cuaterniones con componentes enteros de Z_{256} de modo que cada cuaternión intercambiado conforma una clave de 32 bits. Por ello, para intercambiar claves de 128 bits, se realizan 4 rondas de intercambio.

En [14] se presentó una variante donde las componentes del cuaternión son enteros donde el módulo es 8-bits, 16-bits o 32-bits de modo de adaptar el esquema a las dimensiones del bus de datos del procesador. Así se logró mejorar la eficiencia en el procesamiento gracias a la reducción de cantidad de rondas, logrando mejoras muy importantes en los tiempos de generación de claves.

B. Resumen del Protocolo:

Alice elige dos octoniones aleatorios o_A y o_B, con elementos de $Z_{p=k*8\text{-bits}}$ (con $k = 1, 2$ o 4). Luego elige como clave privada un polinomio entero $f(x)$ con coeficientes y exponentes en Z_{16} tal que $f(o_A) \neq 0$ y dos números enteros aleatorios m y n en Z_{251} y envía a Bob por el canal inseguro los elementos o_A y o_B. Bob elige como clave privada un polinomio entero $h(x)$ con coeficientes y exponentes en Z_{16} tal que $h(o_A) \neq 0$ y dos números enteros aleatorios r y s en Z_{251}. Alice calcula su token: $r_A = f(o_A)^m \,.\, o_B \,.\, f(o_A)^n$. 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). Finalmente: $K_A = K_B$.

La clave obtenida para $k = 1$ posee 8 x 8 bits = 64 bits. Para $k = 2$, la clave posee 8 x 16 bits = 128 bits y para k = 4 posee 8 x 32 = 256 bits. Para lograr una clave de 256 bits [18], el proceso debe repetirse las veces que sea necesario, según cada caso o alternativamente expandir la clave aleatoria usando una función Hashing criptográficamente segura.

La figura 1 muestra un esquema del protocolo propuesto.

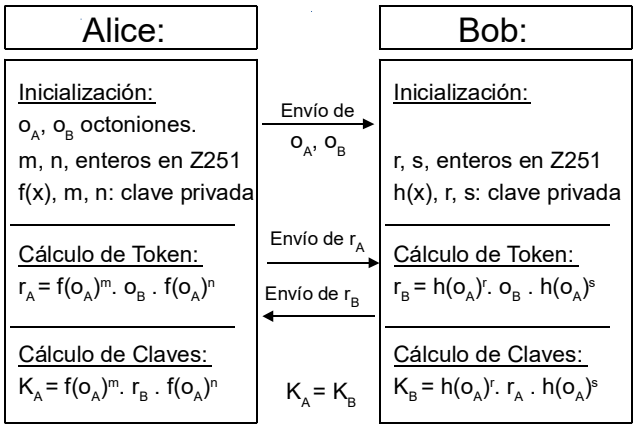

Figura 1: Esquema del protocolo propuesto.

Seguridad Adicional: Si bien el uso tanto de cuaterniones como de octoniones garantiza la aparición de elementos nulos (por formar álgebras de división), y se verifica (dentro del algoritmo) que la valuación de las funciones polinómicas de las claves privadas no sea nula, el álgebra en el anillo de enteros (en las componentes de los octoniones) posee divisores de cero si el módulo no es primo, presentando efectos no deseados. Para evitar este efecto, se trabaja con módulo: el mayor primo menor a K*8 bits. Esto es: si $k = 1$, las componentes del octonion son elementos en Z_{251}, si $k = 2$ sus componentes son elementos en Z_{65521} y si $k = 4$ sus componentes son elementos en $Z_{4294967279}$.

Versiones Propuestas: El protocolo aquí propuesto se presenta en tres versiones: DHECO8 (8 bits), DHECO16 (16 bits) y DHECO32 (32 bits). Las versiones dependen de que cada componente del octonion sea un número entero Z_{251}, Z_{65521} o en

$Z_{4294967279}$. Cada intercambio de claves genera 64 bits, 128 bits o 256 bits. Para obtener claves de 128 bits o 256 bits debe repetirse el proceso las veces que se requiera.

C. Un ejemplo numérico:

Se presenta un ejemplo numérico de la implementación del protocolo propuesto:

Inicialización:

(a) ALICE elige los elementos públicos:

o_A = (157, 188, 177, 188, 203, 149, 217, 148) y o_B = (40, 207, 6, 33, 75, 79, 98, 54).

(b) ALICE elige su clave privada:

Elementos $m = 4$, $n = 122$ y el polinomio $f(x) = 97x^{15} + 98x^{14} + 6x^{13} + 136x^{12} + 238x^{11} + 150x^{10} + 5x^9 + 135x^8 + 186x^7 + 83x^6 + 168x^5 + 90x^4 + 238x^3 + 249x^2 + 150x + 180$.

(c) BOB elige su clave privada:

Elementos $r = 17$, $s = 177$ y el polinomio $h(x) = 157x^{15} + 48x^{14} + 53x^{13} + 124x^{12} + 76x^{11} + 33x^{10} + 166x^9 + 76x^8 + 150x^7 + 52x^6 + 50x^5 + 40x^4 + 114x^3 + 58x^2 + 97x + 5$.

(d) ALICE envía a BOB los octoniones o_A y o_B por el canal inseguro.

Cálculo de tokens:

(e) ALICE calcula su token:

$f(157, 188, 177, 188, 203, 149, 217, 148) = 97.(157, 188, 177, 188, 203, 149, 217, 148)^{15} + 98.(157, 188, 177, 188, 203, 149, 217, 148)^{14} + 6.(157, 188, 177, 188, 203, 149, 217, 148)^{13} + 136.(157, 188, 177, 188, 203, 149, 217, 148)^{12} + 238.(157, 188, 177, 188, 203, 149, 217, 148)^{11} + 150.(157, 188, 177, 188, 203, 149, 217, 148)^{10} + 5.(157, 188, 177, 188, 203, 149, 217, 148)^9 + 135.(157, 188, 177, 188, 203, 149, 217, 148)^8 + 186.(157, 188, 177, 188, 203, 149, 217, 148)^7 + 83.(157, 188, 177, 188, 203, 149, 217, 148)^6 + 168.(157, 188, 177, 188, 203, 149, 217, 148)^5 + 90.(157, 188, 177, 188, 203, 149, 217, 148)^4 + 238.(157, 188, 177, 188, 203, 149, 217, 148)^3 + 249.(157, 188, 177, 188, 203, 149, 217, 148)^2 + 150.(157, 188, 177, 188, 203, 149, 217, 148) + 180.(1, 0, 0, 0, 0, 0, 0, 0) = (161, 14, 128, 14, 178, 190, 147, 246).$

$r_A = (161, 14, 128, 14, 178, 190, 147, 246)^4 . (40, 207, 6, 33, 75, 79, 98, 54) . (161, 14, 128, 14, 178, 190, 147, 246)^{122}$ = (121, 3, 110, 243, 184, 230, 202, 171).

Alice envía a BOB r_A por el canal inseguro.

(f) BOB calcula su token:

$h(157, 188, 177, 188, 203, 149, 217, 148) = 157.(157, 188, 177, 188, 203, 149, 217, 148)^{15} + 48.(157, 188, 177, 188, 203, 149, 217, 148)^{14} + 53.(157, 188, 177, 188, 203, 149, 217, 148)^{13} + 124.(157, 188, 177, 188, 203, 149, 217, 148)^{12} + 76.(157, 188, 177, 188, 203, 149, 217, 148)^{11} + 33.(157, 188, 177, 188, 203, 149, 217, 148)^{10} + 166.(157, 188, 177, 188, 203, 149, 217, 148)^9 + 76.(157, 188, 177, 188, 203, 149, 217, 148)^8 + 150.(157, 188, 177, 188, 203, 149, 217, 148)^7 + 52.(157, 188, 177, 188, 203, 149, 217, 148)^6 + 50.(157, 188, 177, 188, 203, 149, 217, 148)^5 + 40.(157, 188, 177, 188, 203, 149, 217, 148)^4 + 114.(157, 188, 177, 188, 203, 149, 217, 148)^3 + 58.(157, 188, 177, 188, 203, 149, 217, 148)^2 + 97.(157, 188, 177, 188, 203, 149, 217, 148) + 5.(1, 0, 0, 0, 0, 0, 0, 0) = (112, 177, 184, 177, 99, 179, 227, 134).$

$r_B = (112, 177, 184, 177, 99, 179, 227, 134)^{17} . (40, 207, 6, 33, 75, 79, 98, 54) . (112, 177, 184, 177, 99, 179, 227, 134)^{177}$ = (90, 42, 17, 119, 150, 23, 110, 182).

Bob envía a ALICE r_B por el canal inseguro.

Cálculo de Claves de sesión:

(g) ALICE calcula su clave:

$K_A = (161, 14, 128, 14, 178, 190, 147, 246)^4 . (90, 42, 17, 119, 150, 23, 110, 182) . (161, 14, 128, 14, 178, 190, 147, 246)^{122} = (84, 242, 130, 31, 84, 244, 45, 20)$

(h) BOB calcula su clave:

$K_B = (112, 177, 184, 177, 99, 179, 227, 134)^{17} . (121, 3, 110, 243, 184, 230, 202, 171) . (112, 177, 184, 177, 99, 179, 227, 134)^{177} = (84, 242, 130, 31, 84, 244, 45, 20).$

Finalmente: $K_A = (84, 242, 130, 31, 84, 244, 45, 20) = K_B$.

D. Ventajas de la Solución:

Mayor Fortaleza: Los esquemas basados en álgebra no asociativa son más resistentes que los criptosistemas no conmutativos.

Criptosistema Compacto: Al no requerir de librerías de precisión extendida, el esquema propuesto es apto para procesadores de pequeño porte.

Criptosistema Elemental: Como para su implementación se usan solo operaciones suma-producto, no se requiere de ninguna librería específica, lo cual permite que sea implementado con facilidad en dispositivos elementales.

Inmunidad Frente a Ataques de Complejidad Sub-exponencial: La criptografía basada en álgebra no conmutativa es inmune a ataques de complejidad sub-exponencial: a la fecha no se conocen ataques exitosos de este tipo a esta línea criptográfica.

Inmunidad Frente a Ataques de Computadora Cuántica: Visto el estado actual del conocimiento en la materia, se conjetura con suficiente fundamento que el presente protocolo resulta inmune a los ataques cuánticos y de computadoras cuánticas. 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.

Inmunidad Frente a Ataques de Canal Lateral: El flanco débil de los criptosistemas asimétricos actuales en versión de campos conmutativos, es el uso de la optimización *square-and-multiply* (RSA, ElGamal) o *duplicate-and-sum* (Elliptic Curve Cryptography) para las exponenciaciones modulares. Dada la particular estructura de los mismos, los códigos que no hayan sido suficientemente ofuscados, se vuelven sensibles a filtraciones indirectas de sonido, potencia, tiempo, etc. En los protocolos aquí presentados, esa debilidad no existe y por lo tanto no atacables por todas las variantes conocidas de dichas técnicas.

Seguridad y Performance parametrizable: Los elementos secretos m, n, r, s, el grado y los coeficientes de los polinomios que conforman la clave privada son parámetros que pueden variarse convenientemente para ajustar el espacio de claves privadas o bien para mejorar la performance del sistema.

E. Importancia de los Resultados:

La criptografía post-cuántica es un tema de sumo interés mundial: La NIST (*National Institute of Standards and Technology*) ha llamado a presentar propuestas e ideas acerca del tema [30]. Y el modelo aquí propuesto cumple con los requisitos pedidos y será presentado a la citada compulsa.

IV. Resultados Experimentales

A. Resumen del Experimento:

Se analiza la demora promedio en la generación de 1000 claves de 256 bits y se la compara con los otros esquemas basados en matrices y cuaterniones.

B. Equipamiento Usado:

El computador usado contiene un procesador Intel® Core™ i3-2328M CPU @ 2.20GHz × 4 y 3,7 GiB de memoria RAM. Se instaló una distribución GNU/Linux: Kali Rolling 64-bit. Los algoritmos fueron programados en Python 2.7.10. no optimizado.

C. Datos Experimentales:

La Tabla 2 muestra los tiempos de procesamiento para la obtención de 1000 claves para esquemas basados en matrices (DHCM), cuaterniones (DHCQ) y octoniones (DHECO), en módulo 8 bits, 16 bits y 32 bits.

El tiempo promedio (en segundos) para la obtención de 1000 claves con DHCM 8-bits fue 5,1080, con DHCQ 8-bits fue 3,7309, con DHECO 8-bits fue 14,1503 (Tabla 2.a). Para 16 bits los tiempos promedios obtenidos son (Tabla 2.b): 2,6836 para DHCM, 1,8967 para DHCQ y 7,1240 para DHECO. Para 32 bits los resultados obtenidos son (Tabla 2.c): 4,9974 con DHCM, 1,8174 con DHCQ y 4,4769 con DHECO. Como todos los coeficientes de variación (CV) son: CV < 0,1 se acepta al promedio como indicador de tendencia central adecuado.

En este experimento se generaron 90.000 claves sin error.

Tabla 2: Comparación de tiempos de procesamiento para la obtención de 1000 claves de 256 bits con los diferentes esquemas.

	CPU Time (s)		
Nº Test	DHCM8 8-bits	DHCQ8 8-bits	DHECO8 8-bits
1	5.1224	3,8467	14.3885
2	5.3305	3,6249	13.7638
3	5,1230	3,7494	14,2010
4	5,0333	3,7115	14,2701
5	5,1276	3,8629	14,6100
6	5,1235	3,6074	14,4672
7	5,0560	3,6712	13,8587
8	5,1248	3,6755	13,7954
9	5,1232	3,6381	14,0395
10	5,1524	3,9215	13,9608
Promedio	5,1080	3,7309	14,1503
Desvío Std	0,04074	0,11036	0,289798
CV	0,007976	0,02958	0,02048

(a)

	CPU Time (s)		
Nº Test	DHCM16 16-bits	DHCQ16 16-bits	DHECO16 16-bits
1	2,6225	1,8567	7,0445
2	2,7206	1,8486	6,8173
3	2,7336	1,8388	7,1056
4	2,6213	1,8815	7,3024
5	2,5602	1,9452	6,9610
6	2,6352	1,8282	6,9591
7	2,8451	2,0111	6,9750
8	2,6207	1,9776	7,6157
9	2,5583	1,8928	7,2891
10	2,9188	1,8861	7,1700
Promedio	2,6836	1,8967	7,1240
Desvío Std	0,120237	0,061735	0,230857
CV	0,044804	0,03255	0,032406

(b)

	CPU Time (s)		
Nº Test	DHCM32 32-bits	DHCQ32 32-bits	DHECO32 32-bits
1	4,9177	1,7971	4,4477
2	5,0230	1,9950	4,4665
3	4,9549	1,8159	4,4067
4	4,9277	1,8232	4,3853
5	5,0176	1,7477	4,3528
6	4,9433	1,7651	4,4093
7	5,2199	1,8122	4,4480
8	4,9217	1,9134	4,4348
9	5,0184	1,7634	4,9311
10	5,0295	1,7405	4,4869
Promedio	4,9974	1,8174	4,4769
Desvío Std	0,090502	0,080039	0,164403
CV	0,01811	0,044041	0,036722

(c)

V. Conclusiones

El modelo propuesto es inmune a ataques de complejidad sub exponencial. Asimismo, resulta ser robusto frente a ataques de computadora cuántica que empleen el algoritmo de Shor por no emplear campos numéricos, y promete ser en general más resistente que otros modelos basados en álgebra no conmutativa, a pesar de tener mayores tiempos de procesamiento que otros esquemas.

Gracias a no requerir de librerías de precisión extendida, puede implementarse en procesadores de menor porte. Al realizarse íntegramente con operaciones sencillas, su alcance puede extenderse a dispositivos de procesamiento muy elementales.

La posibilidad de poder variar parámetros de la clave privada permite adaptar la solución según las necesidades del usuario de seguridad y performance.

VI. Trabajos Futuros

El modelo propuesto será puesto a pruebas de fortaleza. Se implementarán las versiones del protocolo para 64 bits. Se pretende desarrollar luego un esquema ElGamal basado en esta propuesta.

REFERENCIAS

[1] Marrero Travieso, Yran: La Criptografía como elemento de la seguridad informática. ACIMED 11.6 (2003).

[2] Diffie W., Hellman M.E: New directions in cryptography. IEEE Transactions on information theory, 22, 644-654, (1976).

[3] Menezes, Alfred J., Paul C. Van Oorschot, and Scott A. Vanstone: Handbook of applied cryptography. CRC press (1996).

[4] 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)

[5] Shor P.: Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, SIAM J. Comput., 5, 1484-1509 (1997)

[6] D-Wave-Systems Press Releases [en línea], (2016). Disponible en: <http://www.dwavesys.com/news/press-releases>. Fecha de consulta: 05/06/2016.

[7] IBM: IBM Makes Quantum Computing Available on IBM Cloud to Acceletare Innovation [En Linea], (2016). Disponible en: <https://www-03.ibm.com/ press/ us/ en/ pressrelease/ 49661.wss>. Fecha de consulta: 05/06/2016.

[8] 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)

[9] Shpilrain V., Zapata G.: Combinatorial group theory and public-key cryptography, Preprint arXiv/math.gr, 0410068 (2004)

[10] Barreto,P. et al: Introdução à criptografia pós-quântica, Minicursos do XIII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais, SBSeg, (2013).

[11] Gerritzen L. et al (Editors): Algebraic Methods in Cryptography, Contemporary Mathematics, AMS, Vol. 418, (2006)

[12] Hecht J.: Un modelo compacto de criptografía asimétrica empleando anillos no conmutativos. V Congreso Iberoamericano de Seguridad Informática CIBSI, Montevideo (2009).

[13] Kamlofsky J.A., Hecht J.P, Abdel Masih S., and Hidalgo Izzi, O.: A Diffie-Hellman Compact Model Over Non-Commutative Rings Using Quaternions. VIII Congreso Iberoamericano de Seguridad Informática CIBSI, Quito (2015).

[14] Kamlofsky, J.. "Improving a Compact Cipher Based on Non Commutative Rings of Quaternion". En XXII Congreso Argentino de Ciencias de la Computación, (2016).

[15] Kalka, A., and Teicher, M. "Non-associative key establishment protocols and their implementation." Algebra and Computer Science 677 (2016): 113.

[16] Kalka, A. "Non-associative public-key cryptography", arXiv preprint arXiv:1210.8270, (2012).

[17] Anshel, I., Anshel, M. and Goldfeld, D. "An algebraic method for public-key cryptography", Mathematical Research Letters 6 (1999), 1-5.

[18] Barker E., Roginsky, A. "Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths". NIST Special Publication 800-131A (2015).

[19] ElGamal, Taher. A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms. En Advances in cryptology. Springer Berlin Heidelberg, pp. 10–18 (1984).

[20] Hecht, JP.: Fundamentos de Computación Cuántica. Editorial Académica Española. ISBN 978-3-8484-7529-2 (2005).

[21] 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).

[22] Eftekhari, M.: A Diffie–Hellman key exchange protocol using matrices over non-commutative rings. Groups-Complexity-Cryptology, 4(1), pp. 167–176 (2012).

[23] Hamilton, W. R.: Lectures on Quaternions: Containing a Systematic Statement of a New Mathematical Method, Hodges and Smith, (1853)

[24] Baez, J. The octonions. *Bulletin of the American Mathematical Society* 39.2 (2002): 145-205.

[25] Dixon, G. M. "Division Algebras: Octonions Quaternions Complex Numbers and the Algebraic Design of Physics (Vol. 290)". *Springer Science & Business Media,*(2013).

[26] Woit, P. "String Theory: An Evaluation". *Department of Mathematics, Columbia University .American Scientist, Vol. 90, no.2* (2002).

[27] Baez, John, and John Huerta. "Des octonions pour la théorie des cordes." *Pour la science* 406 (2011): 70-75.

[28] Belousov, V. D. "Moufang loops", *Hazewinkel, Michiel, Encyclopedia of Mathematics, Springer* (2001).

[29] Kamlofsky J., Bergamini L.: Cuaterniones en Visión Robótica. V Congreso de Matemática Aplicada, Computacional e Industrial MACI, Tandil (2015).

[30] 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.

Jorge Kamlofsky. Graduated with a degree in Mathematics in the Universidad Abierta Interamerican (UAI) and a Specialist in Cryptography and IT Security in the Faculty of Engeneering of the Argentinean Army (EST-IUE). He is finishing a Master in IT in the UAI and doing a Doctorate in Engeneering in the Faculty of Engeneering of the National University of Lomas de Zamora (UNLZ). Actually he is profesor of Discrete Mahematics in the UAI and Profesor of Algebta and Analytics Geometry in the National Technological Univertity (UTN). Also he is researcher in the Center of high studies on Information Techology (CAETI).

Pedro Hecht (M'2012). Se graduó como Licenciado en Análisis de Sistemas (ESIO-DIGID), y Doctor de la Universidad de Buenos Aires (UBA). Actualmente es Profesor Titular de Criptografía I y II de la Maestría en Seguridad Informática dependiente de las Facultades de Cs. Económicas, Cs. Exactas y Naturales y de Ingeniería de la Universidad de Buenos Aires (UBA) e idéntico cargo en la Facultad de Ingeniería del Ejército (EST-IUE). Además es el Coordinador Académico de la citada Maestría (UBA), Profesor titular de Biofísica (UBA), Director de proyectos e investigador en modelos matemáticos de UBACyT y Director titular de EUDEBA. Es miembro de Criptored, IEEE Argentina, ACM SIGCSE, ACM SIGITE y otras. Área de interés: álgebra no conmutativa aplicada a la criptografía.

Samira Abdel Masih. Se graduó de Licenciada en Matemática en la Facultad de Matemática, Astronomía y Física de la Universidad Nacional de Córdoba (UNC), y de Doctora en Ciencias Matemáticas en la Facultad de Ciencias Exactas y Naturales de la Universidad de Buenos Aires (UBA). Actualmente es Profesora Titular de Cálculo Infinitesimal II en la Facultad de Tecnología Informática de la Universidad Abierta Interamericana (UAI). También es investigadora en el Centro de Altos Estudios en Tecnología Informática (CAETI), dependiente de la UAI.

.