Artículo Original / Original Research

Ciencias Matemáticas, Vol. 39, No. 1, 2025, Pag. 21-30
Recibido (*Received*): 11-03-2025, Revisado (*Revised*): 16-04-2025
Aceptado (*Accepted*): 12-07-2025, En línea (*Online*): 25-10-2025

Funciones pseudoaleatorias inconscientes en grupos no conmutativos

Oblivious pseudorandom functions in non-commutative groups

David Ricardo Ledo Baster[1]*, Huber Martínez Rodríguez[2]

Resumen Las aplicaciones de las funciones pseudoaleatorias inconscientes en la criptografía y en la seguridad de la información son múltiples. Pueden citarse la derivación de claves basadas en contraseñas, acuerdo de claves basados en contraseñas, *password hardening*, CAPTCHAs imposibles de rastrear, acuerdo de claves homomórfico y la intersección de conjuntos segura. Los primeros trabajos se basan en protocolos para la transferencia inconsciente, computación multiparte segura o en algunas variantes del problema del logaritmo discreto. Recientemente han surgido propuestas postcuánticas basadas en las isogenias de curvas elípticas y en los problemas sobre lattices. En este trabajo se propone el diseño de una función pseudoaleatoria inconsciente que base su seguridad en la dificultad de encontrar el elemento conjugador en grupos no conmutativos. Se realiza además un experimento utilizando como plataforma el grupo discreto de Heisenberg sobre un campo finito.

Palabras Clave: criptografía no conmutativa, elemento conjugador, funciones pseudoaleatorias inconscientes, protocolos criptográficos

Abstract *They are multiple applications of oblivious pseudorandom functions in cryptography and information security. It can be mention the derivation of keys based on passwords, passwords key agreement, password hardening, untraceable CAPTCHAs, homomorphic key agreement, and secure set intersection. The first works are based in protocols for oblivious transfer, secure multiparty computation or in some variants of the discrete logarithm problem. Recently, postquantum proposals have emerged based on the isogenies of elliptic curves and on lattices problems. In this work proposes the design of an oblivious pseudorandom function that bases its security on the difficulty of finding the conjugator element in non-commutative groups. An experiment is also carried out using the discrete Heisenberg group on a finite field as a platform.*

Keywords: *non-commutative cryptography, conjugator element, oblibious pseudorandom functions, cryptographic protocols.*

Mathematics Subject Classification: 20F12, 20F18, 20H20, 94A60.

[1]Departamento de Informática, Universidad de Holguín, Holguín, Cuba. Email: dledob@uho.edu.cu.
[2]Dirección de Ciencia, Tecnología e Innovación, Universidad de Ciego de Ávila Máximo Gómez Báez, Ciego de Ávila, Cuba. Email: martinez.rodriguez.huber@gmail.com.
*__Autor para Correspondencia (*Corresponding Author*)__

Editado por (*Edited by*): Damian Valdés Santiago, Facultad de Matemática y Computación, Universidad de La Habana, La Habana, Cuba.

Citar como: Ledo Baster, D.R., & Martínez Rodríguez, H. (2025). Funciones pseudoaleatorias inconscientes en grupos no conmutativos. *Ciencias Matemáticas*, 39(1), 21–30. DOI: https://doi.org/10.5281/zenodo.17445482. Recuperado a partir de https://revistas.uh.cu/rcm/article/view/11044.

Introducción

La criptografía no conmutativa se basa en estructuras algebraicas como semigrupos, grupos y anillos que no son conmutativos. Una de las primeras aplicaciones de una estructura algebraica no conmutativa con fines criptográficos fue el uso de grupos de trenzas para desarrollar protocolos criptográficos [3, 26]. Posteriormente, se identificaron otras estructuras no conmutativas como grupos de Thompson [36], grupos policíclicos, grupos de Grigorchuk y grupos de matrices [10, 2, 16, 33] como candidatos potenciales para aplicaciones criptográficas. Constituye un área de investigación relativamente jóven y activa desde el año 2000, donde se pueden señalar resultados recientes en [13, 5, 15, 6, 40, 25, 11, 39]. Su

relación con la criptografía postcuántica radica en que ambas buscan establecer algoritmos seguros basados en problemas matemáticos difíciles, pero abordan diferentes contextos y desafíos. Algunos puntos en común son:

1. Uso de estructuras algebraicas:
   - La criptografía basada en grupos utiliza grupos algebraicos para definir problemas complejos, como el logaritmo discreto o problemas en grupos de trenzas.
   - En la criptografía postcuántica, algunos enfoques como los basados en lattices o códigos también dependen de estructuras algebraicas, aunque no exclusivamente de grupos.
2. Resistencia a ataques cuánticos:
   - La criptografía clásica basada en grupos, como Diffie-Hellman o ECC, se ve amenazada por computadoras cuánticas debido al algoritmo de Shor.
   - Esto ha llevado a investigar nuevas variantes de criptografía basada en grupos que sean resistentes a la computación cuántica, como problemas en grupos no conmutativos.
3. Problemas intratables como base de seguridad:
   - Ambas dependen de problemas matemáticos difíciles. La criptografía basada en grupos se centra en problemas como el de la conjugación o el de la palabra.
   - En criptografía postcuántica, se utilizan otros problemas como el aprendizaje con errores (LWE), pero algunos investigadores han explorado problemas sobre grupos que son resistentes a ataques cuánticos.

En el trabajo [23] se detallan algunas de las principales características de la criptografía no conmutativa y se brindan algunos ejemplos. Los autores especifican varios problemas abiertos dentro de los que podemos señalar: la búsqueda de más criptosistemas basados en grupos no conmutativos y su implementación en aplicaciones de la vida real.

Por otra parte, Naor y Reingold [32] notaron que su función pseudoaleatoria (PRF) basada en la teoría de números permite una evaluación interactiva e inconsciente, donde un "cliente" con entrada x obtiene $PRF_k(x)$ para una función $PRF_k(\cdot)$ que es aportada por un "servidor". El cliente no obtiene información sobre el valor k del servidor, ni el servidor obtiene información sobre x ni la salida de la función pseudoaleatoria. Freedman et al. [14] más tarde llamaron a ese protocolo entre dos partes una función pseudoaleatoria inconsciente.

Las aplicaciones de las funciones pseudoaleatorias inconscientes en la criptografía y en la seguridad de la información son múltiples. Podemos citar la derivación de claves basadas en contraseñas, acuerdo de claves basados en contraseñas [20, 22, 21], *password hardening*, CAPTCHAs imposibles de rastrear, acuerdo de claves homomórfico y la intersección de conjuntos segura [17, 27]. Los primeros trabajos se basan en protocolos para la transferencia inconsciente, computación multiparte segura o en algunas variantes del problema del logaritmo discreto.

Recientemente han surgido propuestas postcuánticas basadas en las isogenias de curvas elípticas [4, 8, 30] y en los problemas sobre *lattices* [1].

El problema matemático más empleado en la construcción de protocolos no conmutativos es el problema de búsqueda del conjugador (CSP). Mientras que el problema del logaritmo discreto (DLP) en un grupo G requiere la recuperación del exponente n conociendo g y $h = g^n$, el CSP requiere la recuperación del elemento conjugador $x \in G$ conociendo g y $h = x^{-1}gx$. En muchos casos se utiliza la notación $g^x \backsimeq x^{-1}gx$ lo cual establece una similitud estética entre ambos problemas.

Relevancia del estudio

El aporte principal de este trabajo consiste en el diseño de una función pseudoaleatoria inconsciente y verificable utilizando el grupo discreto de Heisenberg sobre un campo finito. Las alternativas postcuánticas existentes hasta la fecha que utilizan isogenias de curvas elípticas o problemas sobre *lattices* presentan algunas limitaciones relacionadas al tamaño de la prueba que aporta la verificabilidad al protocolo. Se introduce el uso del grupo discreto de Heisenberg como plataforma, aprovechando sus propiedades algebraicas que permiten caracterizar el protocolo propuesto de forma teórica. Por otra parte, el protocolo de conocimiento cero para la igualdad del elemento conjugador que brinda soporte a la función pseudoaleatoria inconsciente, es un aspecto que tiene interés de manera independiente. En esa dirección, la investigación contribuye con el estudio de estructuras matemáticas alternativas especialmente útiles para la seguridad y protección de la información en entornos digitales.

1. Preliminares

1.1 Álgebra abstracta

Definición 1 (Grupo)**.** *Un grupo $(G, *)$ consiste en un conjunto G con una operación binaria $*$ en G que satisface los siguientes tres axiomas:*

1. *Asociatividad:* $\forall a, b, c \in G : a * (b * c) = (a * b) * c$.
2. *Elemento identidad:* $\forall a \in G, \exists\ e \in G : a * e = e * a = a$ *donde e denota el elemento identidad de G.*
3. *Elemento inverso:* $\forall a \in G, \exists\ a^{-1} : a * a^{-1} = a^{-1} * a = 1$ *donde a^{-1} denota el elemento inverso de a.*

Definición 2 (Grupo conmutativo)**.** *Un grupo $(G, *)$ se llama grupo conmutativo o grupo abeliano si además de las*

propiedades de la Definición 1, también se cumple la conmutatividad.

4. ***Conmutatividad**: $\forall a, b \in G : a * b = b * a$.*

Los grupos que cumplen con la Definición 1 y no con la Definición 2 se denominan *grupos no conmutativos*.

Definición 3 (Groupo finito)**.** *Un grupo G es finito si el número de elementos en G denotado $|G|$ es finito. El número de elementos $|G|$ en un grupo finito se llama orden del grupo.*

Definición 4 (Subgrupo)**.** *Dado un grupo $(G, *)$, cualquier H que sea un subconjunto no vacío $H \subseteq G$ y satisfaga los axiomas de un grupo con respecto a la operación de grupo $*$ en H, es un subgrupo de G.*

Lema 1. *Sea $(G, *)$ un grupo. Para los elementos $x, y \in G$, se cumple que $(xy)^{-1} = y^{-1}x^{-1}$.*

Definición 5 (Conjugado)**.** *Sean x y y pertenecientes al grupo $(G, *)$, el elemento $y^{-1}xy$ se conoce como el conjugado de x por y que usalmente se denota por x^y.*

Lema 2. *Sea $(G, *)$ un grupo. Para los elementos $x, y, z \in G$, se cumplen las siguientes afirmaciones:*

1. $(z^x)^y = z^{xy}$,
2. $(z^x)^{-1} = (z^{-1})^x$,
3. *Si $xy = yx$ entonces $(z^x)^y = (z^y)^x$,*
4. $(zy)^x = z^x y^x$.

Las leyes anteriores se derivan directamente del hecho de que la conjugación define una acción de G sobre sí mismo [19].

Las restantes definiciones relacionadas con anillos y campos se pueden encontrar en [28, 18, 34, 35].

1.2 Función pseudoaleatoria inconsciente

Una función pseudoaleatoria inconsciente (OPRF, por sus siglas en inglés, *oblivious pseudorandom function*) es un protocolo entre un Servidor que posee una clave secreta k y un Cliente con una entrada x que permite calcular la salida de una función pseudoaleatoria $y = PRF_k(x)$.

Al finalizar el protocolo:

- El cliente obtiene la salida y de la PRF, y
- **Prueba inconsciente (*obliviousness*)**
  - El Cliente no obtiene ninguna información sobre la clave secreta del Servidor
  - El Servidor no obtiene ninguna información sobre la entrada del cliente ni la salida de la PRF

Función pseudoaleatoria inconsciente verificable Una función pseudoaleatoria inconsciente verificable (VOPRF, por sus siglas en inglés, *verifiable oblivious pseudorandom function*) es una $OPRF$ donde el Cliente puede verificar si el Servidor utilizó una clave específica (Figura 1). El protocolo es correcto si $\mathbf{unblind}(Z) = PRF(k, X)$.

Cliente		Servidor
x entrada		k clave secreta
$X = \mathbf{encode}(x)$	$\xleftarrow{c}$	$c = \mathbf{commit}(k)$
$Y = \mathbf{blind}(X)$	$\xrightarrow{Y}$	$Z = \mathbf{eval}(k, Y)$
	$\xleftarrow{(Z,\pi)}$	$\pi = \mathbb{P}(k, c, Y, Z)$
Si $1 = \mathbb{V}(\pi, c, Y, Z)$ return $\mathbf{unblind}(Z)$		

Figura 1. función pseudoaleatoria inconsciente verificable [*Verifiable oblivious pseudorandom function*].

1.3 Teoría de la probabilidad

En esta sección se introduce la terminología básica sobre teoría de la probabilidad.

Definición 6 (Experimento [29])**.** *Un experimento es un procedimiento que produce uno de un conjunto de resultados dados. El conjunto de todos los resultados posibles se llama espacio muestral S.*

Definición 7 (Distribución de probabilidad [29])**.** *Una distribución de probabilidad P sobre S es una secuencia de números $p_1, p_2, \cdots, p_n$, que son todos no negativos y suman uno. El número p_i se interpreta como la probabilidad de que s_i sea el resultado del experimento, tal que $Pr[s_i] = p_i$.*

Definición 8 (Variable aleatoria [29])**.** *Una variable aleatoria X es una función del espacio muestral S al conjunto de números reales; a cada evento simple $s_i \in S$, X le asigna un número real $X(s_i)$.*

Definición 9 (Conjunto de variables aleatorias)**.** *Un conjunto de variables aleatorias es un conjunto de variables aleatorias indexadas $E_X = \{X_1, \ldots, X_n\}, n \in \mathbb{N}$.*

Definición 10 (Aleatoriedad perfecta)**.** *Una secuencia de bits w contiene aleatoriedad perfecta o se dice que es elegida uniformemente aleatoria si cada bit b en w podría haber sido el resultado del lanzamiento de una moneda justa. Es decir, la probabilidad de que $b = 1$ sea igual a la probabilidad de $b = 0$ o más formalmente, $Pr[b = 1] = Pr[b = 0] = \frac{1}{2}$. De modo que una secuencia de bits es un conjunto de variables aleatorias donde cada variable aleatoria representa un bit.*

Definición 11 (Distribución de probabilidad invariante a la multiplicación por la izquierda)**.** *Sea $(G, *)$ un grupo y la distribución de probabilidad P definida sobre G. Sea el evento E que consiste en seleccionar un elemento $e \in G$.*

Si se cumple que $P(E) = P(\{ax \mid \forall a \in G\})$ se dice que la distribución de probabilidad es invariante a la multiplicación por la izquierda.

1.4 Protocolos Sigma (Σ-*Protocols*)

La siguiente sección presenta los protocolos Σ, y su definición de seguridad. Un excelente complemento de los protocolos Σ aparece en el libro de Boneh y Shoup [9].

Los protocolos Σ son protocolos bipartitos en forma de tres movimientos, con un problema computacionalmente difícil que define la relación R, tal que $(h, w) \in R$ si h es una instancia del problema, y w es la solución a h. Esta relación también se puede expresar como una función, tal que $(h, w) \in \mathrm{R} \iff \mathrm{R}_f\ h\ w = 1$.

Un protocolo Σ permite a un probador convencer al verificador de que conoce w, sin revelarle nunca w. En la Figura 2 se puede ver una descripción general de un protocolo Σ.

Probador		Verificador
(h, w)		h
$a = commit(h, w)$	$\xrightarrow{a}$	
$z = response(h, w, a, e)$	$\xleftarrow{e}$	$e \leftarrow \{0,1\}^*$
	$\xrightarrow{z}$	$verify(h, a, e, z)$

Figura 2. Protocolo Σ [Σ-*Protocol*].

Se observa que el protocolo tiene una forma de tres movimientos, ya que solo se envían tres mensajes, (a, e, z), entre el probador y el verificador.

Seguridad Se dice que un protocolo Σ es seguro si satisface las siguientes definiciones.

Definición 12 (*Completness*)**.** *Suponiendo que tanto P como V son honestos i. e. siguiendo el protocolo, entonces V siempre* ***aceptará*** *al final del protocolo.*

Definición 13 (*Special soundness*)**.** *Dado un protocolo Σ S para alguna relación R con entrada pública h y dos transcripciones que acepten (a, e, z) y (a, e', z') donde ambas transcripciones tienen el mismo mensaje inicial, a y $e \neq e'$. Entonces S satisface la propiedad* special soundness *si existe un algoritmo llamado "extractor de testigos", que dadas dos transcripciones, se obtiene un testigo válido para la relación R.*

La propiedad *special soundness* es importante para garantizar que un probador que hace trampa no puede convencer de manera confiable al verificador. Dada la propiedad *special soundness*, la probabilidad de que un probador tramposo pueda convencer al verificador es insignificante si el protocolo se corre varias veces. *special soundness* implica que sólo existe un desafío, para cualquier mensaje dado a, que puede hacer que el protocolo sea aceptado, sin conocer el testigo. Por lo tanto, dado un espacio de desafío con cardinalidad c la probabilidad de que un probador tramposo tenga éxito en convencer al verificador es $\frac{1}{c}$. Luego, el protocolo se puede ejecutar varias veces para hacer que su probabilidad sea $(\frac{1}{c})^n$, donde n es el número de ejecuciones.

La definición de *special soundness* también se puede generalizar a s-*special soundness*. Esta definición requiere que el testigo pueda construirse, dado s transcripciones aceptadas.

Definición 14 (*Special honest-verifier zero-knowledge*)**.** *Un Σ-Protocol S se dice que es SHVZK si existe un algoritmo Sim polinomial, que dada la instancia h y el desafío e como entrada produce una transcripción (a, e, z) indistinguible de la transcripción producida por S.*

Los $\Sigma - Protocol$ permiten construir protocolos de conocimiento cero, seguros en el modelo del oráculo aleatorio, y sin cálculos adicionales. Esto efectivamente permite construir un protocolo seguro de conocimiento cero y solo tener que demostrar que el protocolo es de conocimiento cero en el caso de un verificador honesto. Esta transformación desde un $\Sigma - Protocol$ de conocimiento cero se conoce como "la transformación de Fiat-Shamir". Más detalles sobre esta transformación se pueden encontrar en la sección 1.4.1.

1.4.1 Transformación Fiat-Shamir

La transformación Fiat-Shamir es una técnica para convertir protocolos Σ en protocolos de conocimiento cero. Los protocolos Σ casi satisfacen la definición de conocimiento cero, el único problema es que los protocolos Σ sólo garantizan conocimiento cero en presencia de un verificador honesto. Sin embargo, si podemos alterar ligeramente el protocolo para obligar al verificador a ser siempre honesto, entonces el protocolo, por definición, debe ser de conocimiento cero. La transformación Fiat-Shamir logra esto eliminando el verificador del protocolo, haciéndolo así no interactivo. El verificador es reemplazado por un oráculo aleatorio, que genera un valor uniformemente aleatorio normalmente utilizando una función Hash.

2. Prueba de igualdad del conjugador

Basado en el protocolo de autenticación desarrollado en [37] y el protocolo de Chaum-Pedersen [12] para la igualdad del logaritmo discreto, se propone un protocolo para comprobar la igualdad del elemento conjugador denominado $\mathbb{CEQT}$[1] por sus siglas en inglés. Para ello establecemos la relación siguiente: $R_{CEQT} = \{(x; (y_1, g_1, y_2, g_2)) | y_1 = g_1^x \wedge y_2 = g_2^x\}$. En el protocolo $\mathbb{CEQT}$ de la Figura 3, la selección de r se realiza utilizando una distribución de probabilidad P invariante a la multiplicación por la izquierda. Además, si la salida $v = 1$ el verificador acepta, en caso contrario aborta.

Teorema 1 (*Completness*)**.** *El protocolo $\mathbb{CEQT}$ es correcto.*

Demostración. Para el caso en el que el verificador seleccione $c = 0$, la validación $a_1 = g_1^s \wedge a_2 = g_2^s$ es trivial porque el probador envió exactamente el valor de r en la variable s. Cuando $c = 1$ se tiene que $a_1 = g_1^r = g_1^{xx^{-1}r} = (g_1^x)^{x^{-1}r} = y_1^{x^{-1}r}$ aplicando las propiedades del lema 2, y como $x^{-1}r = s$ la validación funciona también. □

Teorema 2 (*Special soundness*)**.** *El protocolo $\mathbb{CEQT}$ posee la propiedad special soundness.*

Demostración. Sean dos transcripciones (a, e, z) y (a, e', z') utilizando la notación de la definición 13. Como son válidas y deben cumplir que $e \neq e'$, entonces tenemos que $a =$

[1] Conjugator Equality Test

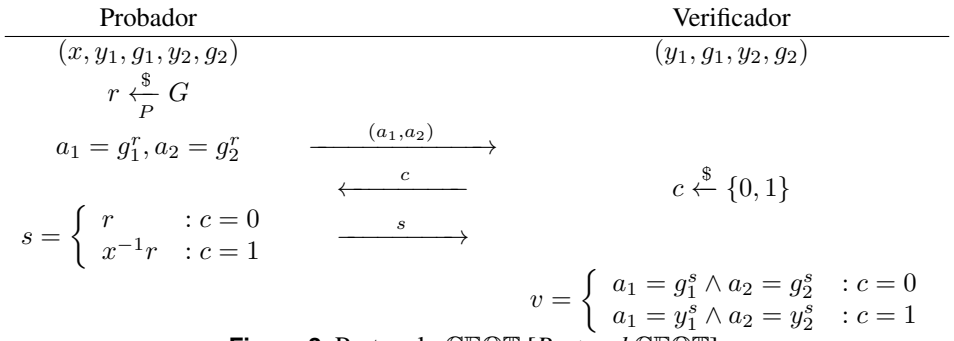

Figura 3. Protocolo $\mathbb{CEQT}$ [*Protocol* $\mathbb{CEQT}$].

$(a_1, a_2), e = 0, e' = 1, z = r, z' = x^{-1}r$, por lo tanto $x = (z'z^{-1})^{-1} = zz'^{-1}$ y queda definido el testigo. □

Teorema 3 (SHVZK)**.** *El protocolo* $\mathbb{CEQT}$ *posee la propiedad SHVZK.*

Demostración. Considere un simulador simple que, al ingresar $h \in G$ y un desafío c, genere lo siguiente.

- Cuando $c = 0$, se elige $h \xleftarrow{\$} G$ y se devuelve (g_1^h, g_2^h) y h. La transcripción resultante es exactamente la de una ejecución honesta del protocolo.
- Cuando $c = 1$, se elige $h \xleftarrow{\$} G$ y se devuelve (y_1^h, y_2^h) y h. La transcripción resultante conduce a una distribución que es la misma que la de la transcripción obtenida ejecutando honestamente el protocolo. Esto se debe a que la distribución de probabilidad es invariante a la multiplicación por la izquierda, por lo que como h y r son elegidos de la misma distribución entonces h y $x^{-1}r$ también cumplen con la misma distribución.

□

En el protocolo se puede aplicar la tansformación de Fiat-Shamir para convertirlo en un protocolo no interactivo. Utilizando una función hash criptográfica, por ejemplo SHA-2, para generar un único bit pseudoaleatorio que simula el bit $c \xleftarrow{\$} \{0, 1\}$ generado por el verificador. El proceso implica proporcionar una entrada única a la función hash y extraer un bit de la salida. Los pasos para lograrlo serían:

1. Entrada: La tupla (a_1, a_2).
2. Hash de la entrada: Se calcula el hash utilizando la función hash segura.
3. Extracción de un bit: Devolver el bit menos significativo del primer byte de la salida de la función hash.

3. Función pseudoaleatoria inconsciente y verificable

El diseño de la función pseudoaleatoria inconsciente verificable de este trabajo está motivado principalmente por las ideas de Jarecki et al. [20] y Albrecht et al. [1].

Sea el grupo multiplicativo $(G, *)$ no conmutativo, un elemento $a \in G$ y dos subconjuntos no vacíos $A \subset G$ y $B \subset G$ tales que $\forall a \in A, \forall b \in B : ab = ba$. El protocolo de la Figura 4 describe la función pseudoaleatoria inconsciente verificable propuesta en este trabajo.

Teorema 4 (*Completeness*)**.** *El protocolo de la Figura 4 es correcto.*

Demostración. Sustituyendo valores y aplicando las propiedades del lema 2, $Z(c^{-1})^r = (Xa^r)^k(c^{-1})^r = X^k a^{rk}(c^r)^{-1} = X^k a^{rk}(a^{kr})^{-1}$. Como los valores de r y k conmutan, entonces $Z(c^{-1})^r = X^k a^{rk}(a^{rk})^{-1} = X^k$. □

4. Implementación utilizando el grupo discreto de Heisenberg

Los grupos de Heisenberg han sido ampliamente estudiados desde el punto de vista del análisis, geometría, física, etc. Desde el punto de vista de la teoría de grupos a menudo se utilizan como ejemplos de grupos nilpotentes, lo que implica que son policíclicos. En el libro de Binz et al. [7] se detallan otras propiedades. El grupo tridimensional de Heisenberg, a menudo conocido como grupo de Heisenberg, es el grupo de matrices triangulares superiores de 3×3 de la forma:

$$\begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix},$$

donde $x, y, z \in \mathbb{R}$. Generalizando el grupo de Heisenberg, tenemos grupos de Heisenberg de dimensiones superiores, $H^{2n+1}, n \geqslant 1, n \in \mathbb{Z}$. Como grupo de matrices, son grupos de dimensión $n + 2$ de la forma:

$$\begin{pmatrix} 1 & x_1 & \cdots & x_n & z \\ 0 & 1 & 0 & \cdots & y_1 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & y_n \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix},$$

donde $x_i, y_i, z \in \mathbb{F}$ siendo $\mathbb{F}$ un campo. En este trabajo utilizaremos campos finitos, lo cual los convierte en grupos discretos finitos.

Cliente		Servidor
$x \in \{0,1\}^*$ entrada		$k \in B$ clave secreta
$X = \mathbf{Hash}(x) \in G$		
$r \xleftarrow{\$} A$	$\xleftarrow{c}$	$c = a^k$
$Y = Xa^r$	$\xrightarrow{Y}$	
		$Z = Y^k$
		$\pi = \mathbb{P}_{\mathbb{CEQT}}(k, c, Y, Z)$
	$\xleftarrow{(Z,\pi)}$	
Si $1 = \mathbb{V}_{\mathbb{CEQT}}(\pi, c, Y, Z)$		
return $Z(c^{-1})^r$		

Figura 4. Protocolo $OVPRF$ [*Protocol* $OVPRF$].

Sea el grupo de Heisenberg $H^{2n+1}(\mathbb{F}_{p^m})$, sus elementos se pueden representar por:

$$\begin{pmatrix} 1 & \mathbf{x} & z \\ 0 & I_n & \mathbf{y} \\ 0 & 0 & 1 \end{pmatrix},$$

donde $\mathbf{x}$ es un vector fila de longitud n, $\mathbf{y}$ es un vector columna de longitud n y I_n es la matriz identidad de dimensión n. Su estructura de grupo queda determinada por:

$$\begin{pmatrix} 1 & \mathbf{x} & z \\ 0 & I_n & \mathbf{y} \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & \mathbf{x}' & z' \\ 0 & I_n & \mathbf{y}' \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & \mathbf{x}+\mathbf{x}' & z+z'+\mathbf{x}\cdot\mathbf{y}' \\ 0 & I_n & \mathbf{y}+\mathbf{y}' \\ 0 & 0 & 1 \end{pmatrix} \tag{1}$$

$$\begin{pmatrix} 1 & \mathbf{x} & z \\ 0 & I_n & \mathbf{y} \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & -\mathbf{x} & -z+\mathbf{x}\cdot\mathbf{y} \\ 0 & I_n & -\mathbf{y} \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & I_n & 0 \\ 0 & 0 & 1 \end{pmatrix} \tag{2}$$

Sea el subconjunto A de $H^{2n+1}(\mathbb{F}_{p^m})$ con $n \geq 2$ donde los elementos están definidos por:

$$\begin{pmatrix} 1 & \mathbf{x} & z \\ 0 & I_n & \mathbf{y} \\ 0 & 0 & 1 \end{pmatrix},$$

con $z \in \mathbb{F}_{p^m}, x = (0, 0, \cdots, a), a \in \mathbb{F}_{p^m}$ y $y = (b, 0, \cdots, 0)^\top, b \in \mathbb{F}_{p^m}$.

Lema 3. *El subconjunto A es un subgrupo de $H^{2n+1}(\mathbb{F}_{p^m})$ isomorfo al grupo aditivo de $\mathbb{F}_{p^m}^3$.*

Demostración. Utilizando la ecuación 1 el producto de dos elementos queda determinado por:

$$\begin{pmatrix} 1 & \mathbf{x}+\mathbf{x}' & z+z' \\ 0 & I_n & \mathbf{y}+\mathbf{y}' \\ 0 & 0 & 1 \end{pmatrix} \in A,$$

y el inverso lo determina la ecuación 2 donde queda la matriz:

$$\begin{pmatrix} 1 & -\mathbf{x} & -z \\ 0 & I_n & -\mathbf{y} \\ 0 & 0 & 1 \end{pmatrix} \in A,$$

lo cual establece que A es un subgrupo. Sea $(a, b, c) \in \mathbb{F}_{p^m}^3$, la construcción $\mathbf{x} = (0, 0, \cdots, a)$ y $\mathbf{y} = (c, 0, \cdots, 0)^\top$:

$$\begin{pmatrix} 1 & \mathbf{x} & b \\ 0 & I_n & \mathbf{y} \\ 0 & 0 & 1 \end{pmatrix},$$

establece un isomorfismo de manera trivial. □

Lema 4. *El subconjunto A es un subgrupo conmutativo de $H^{2n+1}(\mathbb{F}_{p^m})$.*

Demostración. El producto se determina por:

$$\begin{pmatrix} 1 & \mathbf{x} & z \\ 0 & I_n & \mathbf{y} \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & \mathbf{x}' & z' \\ 0 & I_n & \mathbf{y}' \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & \mathbf{x}+\mathbf{x}' & z+z'+\mathbf{x}\cdot\mathbf{y}' \\ 0 & I_n & \mathbf{y}+\mathbf{y}' \\ 0 & 0 & 1 \end{pmatrix},$$

pero $\mathbf{x} \cdot \mathbf{y}' = 0$ por la propia construcción de los vectores.

Al invertir el orden de las matrices:

$$\begin{pmatrix} 1 & \mathbf{x}' & z' \\ 0 & I_n & \mathbf{y}' \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & \mathbf{x} & z \\ 0 & I_n & \mathbf{y} \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & \mathbf{x}' + \mathbf{x} & z' + z + \mathbf{x}' \cdot \mathbf{y} \\ 0 & I_n & \mathbf{y}' + \mathbf{y} \\ 0 & 0 & 1 \end{pmatrix},$$

y como también se cumple que $\mathbf{x}' \cdot \mathbf{y} = 0$, se garantiza que el producto sea conmutativo. □

Lema 5. *La distribución uniforme en $H^{2n+1}(\mathbb{F}_{p^m})$ es invariante a la multiplicación por la izquierda.*

Demostración. Cada elemento de $H^{2n+1}(\mathbb{F}_{p^m})$ se puede escribir como un vector fila $(x_1, \ldots, x_n, z, y_1, \ldots, y_n)$ resumido como $(\mathbf{x}, z, \mathbf{y})$. El producto por la izquierda se puede reescribir como:

$$(\mathbf{a}, z', \mathbf{b})(\mathbf{x}, z, \mathbf{y}) = (\mathbf{a} + \mathbf{x}, z' + z + \mathbf{a} \cdot \mathbf{y}, \mathbf{b} + \mathbf{y}).$$

Si $(\mathbf{a}, z', \mathbf{b})$ es constante y $(\mathbf{x}, z, \mathbf{y})$ es elegido mediante la selección de $2n + 1$ variables aleatorias independientes y uniformemente distribuidas en $\mathbb{F}_{p^m}$, teniendo en cuenta que en un campo finito la suma y el producto por una constante son automorfismos, y que la suma de variables aleatorias uniformes da como resultado una variable aleatoria uniforme, se puede concluir el resultado. □

El lema 5 garantiza que la selección uniforme se pueda utilizar en el protocolo de la Figura 3. En el caso del lema 4, nos permite establecer los subconjuntos desde donde se eligen los valores para r y k respectivamente en el protocolo de la Figura 4.

Algunas consideraciones de seguridad En [31] los autores especulan sobre la posibilidad de utilizar los grupos de matrices como plataforma para desarrollar criptosistemas no conmutativos. En el caso específico del grupo de Heisenberg, en [24] se realiza un experimento donde se demuestra la resistencia a los ataques por longitud de la palabra en el criptosistema de Anshel-Anshel-Goldfeld convirtiéndolo en una opción más segura al grupo de trenzas en las que originalmente se basa el protocolo. El trabajo de [38] investiga la complejidad del problema de búsqueda del conjugador en grupos policíclicos y grupos de matrices. En este caso, diseñan un algoritmo polinomial para resolver el problema de búsqueda del conjugador en p-grupos extraespeciales. En el caso particalar de los protocolos propuestos en este trabajo, podemos evitarlo utilizando el grupo $H^{2n+1}(\mathbb{F}_{p^m})$ con $m \geqslant 2$.

Conclusiones

Con la investigación se diseñó un protocolo para una función pseudoaleatoria inconsciente y verificable que basa su seguridad en la dificultad de encontrar el elemento conjugador en un grupo no conmutativo. El grupo discreto de Heisenberg sobre un campo finito posee propiedades interesantes que pueden ser aprovechadas en el campo de la criptografía no conmutativa. Su instanciación utilizando campos finitos permite trabajar con la distribución de probabilidad uniforme de manera natural, lo cual es muy importante en temas de seguridad criptográfica. Esto garantiza que sea una alternativa para utilizar como plataforma en protocolos tipo OVPRF.

Trabajo futuro

Algunos aspectos necesitan seguir desarrollándose para fortalecer la investigación. Por ejemplo, estimar concretamente los parámetros para su funcionamiento en aplicaciones de la vida real y optimizar el protocolo de conocimiento cero para la igualdad del conjugador. En esta dirección sería interesante aumentar el tamaño del conjunto desde donde el verificador genera los retos. Además, analizar la posibilidad de utilizar variantes infinitas del grupo discreto de Heisenberg. Esto podría imponer retos importantes desde el punto de vista del tamaño de los parámetros y/o para la selección aleatoria de los elementos.

Suplementos

Este artículo no contiene información suplementaria.

Conflictos de interés

Los autores declaramos que no tenemos ningún conflicto de interés en relación con este artículo. No hubo ninguna subvención para este artículo.

Contribución de autoría

Conceptualización D.R.L.B., H.M.R.

Análisis formal D.R.L.B.

Investigación D.R.L.B., H.M.R.

Supervisión H.M.R.

Validación D.R.L.B., H.M.R.

Visualización D.R.L.B.

Redacción: preparación del borrador original D.R.L.B.

Redacción: revisión y edición H.M.R.

Referencias

[1] Albrecht, M.R., A. Davidson, A. Deo, and N.P. Smart: *Round-optimal verifiable oblivious pseudorandom functions from ideal lattices*. In Garay, J.A. (editor): *Public-Key Cryptography – PKC 2021*, pages 261–289, Cham, 2021. Springer International Publishing, ISBN 978-3-030-75248-4. https://doi.org/10.1007/978-3-030-75248-4_10.

[2] Anjaneyulu, G.S.G.N., P.V. Reddy, and U.M. Reddy: *Secured digital signature scheme using polynomials over non-commutative division semirings*. International Journal of Computer Science and Network Security, 8(8):278, 2008. http://paper.ijcsns.org/07_book/200808/20080839.pdf.

[3] Anshel, I., M. Anshel, and D. Goldfeld: *An algebraic method for public-key cryptography*. Mathematical Research Letters, 6:287–291, 1999. https://api.semanticscholar.org/CorpusID:11621019.

[4] Basso, A.: *A post-quantum round-optimal oblivious prf from isogenies*. In *Selected Areas in Cryptography - SAC 2023: 30th International Conference, Fredericton, Canada, August 14-18, 2023, Revised Selected Papers*, pages 147–168, Berlin, Heidelberg, 2024. Springer-Verlag, ISBN 978-3-031-53367-9. https://doi.org/10.1007/978-3-031-53368-6_8.

[5] Battarbee, C., D. Kahrobaei, L. Perret, and S.F. Shahandashti: *Spdh-sign: towards efficient, post-quantum group-based signatures*. In *International Conference on Post-Quantum Cryptography*, pages 113–138. Springer, 2023. https://doi.org/10.1007/978-3-031-40003-2_5.

[6] Battarbee, C., D. Kahrobaei, L. Perret, and S.F. Shahandashti: *A subexponential quantum algorithm for the semidirect discrete logarithm problem*. In *International Conference on Post-Quantum Cryptography*, pages 202–226. Springer, 2024. https://doi.org/10.1007/978-3-031-62743-9_7.

[7] Binz, E. and S. Pods: *The Geometry of Heisenberg Groups: With Applications in Signal Theory, Optics, Quantization, and Field Quantization*. Mathematical surveys and monographs. American Mathematical Society, 2008, ISBN 9780821844953. https://books.google.com.cu/books?id=yIP0BwAAQBAJ.

[8] Boneh, D., D. Kogan, and K. Woo: *Oblivious pseudorandom functions from isogenies*. In Moriai, S. and H. Wang (editors): *Advances in Cryptology – ASIACRYPT 2020*, pages 520–550. Springer International Publishing, 2020, ISBN 978-3-030-64834-3. https://doi.org/10.1007/978-3-030-64834-3_18.

[9] Boneh, D. and V. Shoup: *A graduate course in applied cryptography*, 2023. https://toc.cryptobook.us/book.pdf.

[10] Cao, Z., X. Dong, and L. Wang: *New public key cryptosystems using polynomials over non-commutative rings*. IACR Cryptol. ePrint Arch., 2007:9, 2007. https://api.semanticscholar.org/CorpusID:14026951.

[11] Carvalho, A. and A. Malheiro: *Subsets of groups in public-key cryptography*. Advances in Mathematics of Communications, 19(3):980–995, 2025, ISSN 1930-5346. https://doi.org/10.3934/amc.2024036.

[12] Chaum, D. and T.P. Pedersen: *Wallet databases with observers*. In Brickell, E.F. (editor): *Advances in Cryptology – CRYPTO' 92*, pages 89–105, Berlin, Heidelberg, 1993. Springer Berlin Heidelberg, ISBN 978-3-540-48071-6. https://doi.org/10.1007/3-540-48071-4_7.

[13] Cumplido, M., D. Kahrobaei, and M. Noce: *The root extraction problem in braid group-based cryptography*. La Matematica, 3(3):1207–1217, 2024. https://link.springer.com/content/pdf/10.1007/s44007-024-00117-x.pdf.

[14] Freedman, M.J., Y. Ishai, B. Pinkas, and O. Reingold: *Keyword search and oblivious pseudorandom functions*. In Kilian, J. (editor): *Theory of Cryptography*, pages 303–324, Berlin, Heidelberg, 2005. Springer Berlin Heidelberg, ISBN 978-3-540-30576-7. https://doi.org/10.1007/978-3-540-30576-7_17.

[15] González Vasco, M.I., D. Kahrobaei, and E. McKemmie: *Applications of finite non-abelian simple groups to cryptography in the quantum era*. La Matematica, 3(2):588–603, 2024. https://doi.org/10.1007/s44007-024-00096-z.

[16] Grigoriev, D. and I. Ponomarenko: *Constructions in public-key cryptography over matrix groups*, 2005. https://hal.science/hal-03047011/document.

[17] Hazay, C. and Y. Lindell: *Efficient protocols for set intersection and pattern matching with security against malicious and covert adversaries*. In Canetti, R. (editor): *Theory of Cryptography*, pages 155–175, Berlin, Heidelberg, 2008. Springer Berlin Heidelberg, ISBN 978-3-540-78524-8. https://doi.org/10.1007/978-3-540-78524-8_10.

[18] Herstein, I.N.: *Álgebra Moderna*. Trillas, 2nd edition, 2012. https://www.academia.edu/14931038/Algebra_Moderna_Herstein.

[19] Hungerford, T.W.: *Groups*, pages 23–69. Springer New York, New York, 1974, ISBN 978-1-4612-6101-8. https://doi.org/10.1007/978-1-4612-6101-8_2.

[20] Jarecki, S., A. Kiayias, and H. Krawczyk: *Round-Optimal Password-Protected Secret Sharing and T-PAKE in the Password-Only Model*. In Sarkar, P. and T. Iwata (editors): *Advances in Cryptology – ASIACRYPT 2014*, pages 233–253, Berlin, Heidelberg, 2014. Springer Berlin Heidelberg, ISBN 978-3-662-45608-8. https://doi.org/10.1007/978-3-662-45608-8_13.

[21] Jarecki, S., H. Krawczyk, and J. Resch: *Updatable Oblivious Key Management for Storage Systems*. In *CCS*

'19: Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, pages 379–393, New York, NY, USA, 2019. Association for Computing Machinery, ISBN 9781450367479. https://doi.org/10.1145/3319535.3363196.

[22] Jarecki, S., H. Krawczyk, and J. Xu: *OPAQUE: An Asymmetric PAKE Protocol Secure Against Pre-computation Attacks*. In Nielsen, J.B. and V. Rijmen (editors): *Advances in Cryptology – EUROCRYPT 2018*, pages 456–486, Cham, 2018. Springer International Publishing, ISBN 978-3-319-78372-7. https://doi.org/10.1007/978-3-319-78372-7_15.

[23] Kahrobaei, D., R. Flores, and M. Noce: *Group-based cryptography in the quantum era*. Cryptology ePrint Archive, Paper 2022 1161, 2022. https://eprint.iacr.org/2022/1161.

[24] Kahrobaei, D. and H.T. Lam: *Heisenberg groups as platform for the aag key-exchange protocol*. In *2014 IEEE 22nd International Conference on Network Protocols*, pages 660–664, 2014. https://doi.org/10.1109/ICNP.2014.105.

[25] Kahrobaei, D., M. Noce, and E. Rodaro: *Applications of automaton groups in cryptography*. International Journal of Computer Mathematics: Computer Systems Theory, 9(2):96–106, 2024. https://doi.org/10.1080/23799927.2024.2335157.

[26] Ko, K.H., S.J Lee, J.H. Cheon, J.W. Han, J. Kang, and C. Park: *New Public-Key Cryptosystem Using Braid Groups*. In Bellare, M. (editor): *Advances in Cryptology – CRYPTO 2000*, pages 166–183, Berlin, Heidelberg, 2000. Springer Berlin Heidelberg, ISBN 978-3-540-44598-2. https://doi.org/10.1007/3-540-44598-6_10.

[27] Kolesnikov, V., R. Kumaresan, M. Rosulek, and N. Trieu: *Efficient batched oblivious prf with applications to private set intersection*. In *Proceedings of the ACM Conference on Computer and Communications Security*, pages 818–829. Association for Computing Machinery, 2016. https://doi.org/10.1145/2976749.2978381.

[28] Kostrikin, A.I.: *Introducción al álgebra*. Mir, 1983. https://archive.org/details/kostrikin-introduccion-al-algebra-mir-1983.

[29] Menezes, A., P.C. van Oorschot, and S.A. Vanstone: *Handbook of Applied Cryptography*. CRC Press, 1996, ISBN 0-8493-8523-7. https://theswissbay.ch/pdf/Gentoomen%20Library/Cryptography/Handbook%20of%20Applied%20Cryptography%20-%20Alfred%20J.%20Menezes.pdf.

[30] Moriya, T., H. Onuki, and T. Takagi: *Sigamal: A supersingular isogeny-based pke and its application to a prf*. In *Advances in Cryptology - ASIACRYPT 2020: 26th International Conference on the Theory and Application of Cryptology and Information Security, Daejeon, South Korea, December 7-11, 2020, Proceedings, Part II*, pages 551–580, Berlin, Heidelberg, 2020. Springer-Verlag, ISBN 978-3-030-64833-6. https://doi.org/10.1007/978-3-030-64834-3_19.

[31] Myasnikov, A., V. Shpilrain, and A. Ushakov: *Non-Commutative Cryptography and Complexity of Group-Theoretic Problems*. American Mathematical Society, USA, 2011, ISBN 0821853600. https://dl.acm.org/doi/10.5555/2161874.

[32] Naor, M. and O. Reingold: *Number-theoretic constructions of efficient pseudo-random functions*. In *Proceedings 38th Annual Symposium on Foundations of Computer Science*, pages 458–467, 1997. https://doi.org/10.1109/SFCS.1997.646134.

[33] Pan, P., L. Wang, L. Wang, L. Li, and Y. Yang: *CSP-DHIES: a new public-key encryption scheme from matrix conjugation*. Security and Communication Networks, 5(7):809–822, 2012. https://doi.org/10.1002/sec.376.

[34] Rotman, J.J.: *Advanced Modern Algebra*. Prentice Hall, 2nd edition, 2003. https://share.google/aCcDkPO1CbxXLIACh.

[35] Shoup, V.: *A Computational Introduction to Number Theory and Algebra*. Cambridge University Press, 2nd edition, 2009. https://shoup.net/ntb.

[36] Shpilrain, V. and A. Ushakov: *Thompson's Group and Public Key Cryptography*. In Ioannidis, J., A. Keromytis, and M. Yung (editors): *Applied Cryptography and Network Security*, pages 151–163, Berlin, Heidelberg, 2005. Springer Berlin Heidelberg, ISBN 978-3-540-31542-1. https://doi.org/10.1007/11496137_11.

[37] Sibert, H., P. Dehornoy, and M. Girault: *Entity authentication schemes using braid word reduction*. Discrete Applied Mathematics, 154(2):420–436, 2006, ISSN 0166-218X. https://doi.org/10.1016/j.dam.2005.03.015, Coding and Cryptography.

[38] Tinani, S., C. Matteotti, and J. Rosenthal: *Cryptanalysis of some nonabelian group-based key exchange protocols*, 2023. https://arxiv.org/abs/2203.03525.

[39] Wang, T. and Z. Xu: *The application of group theory behind modern cryptography*. Theoretical and Natural Science, 13:195–201, 2023. https://doi.org/10.54254/2753-8818/13/20240844.

[40] Zhao, M., H. Wang, and B. Yao: *Graphic groups, graph homomorphisms, and graphic group lattices in asymmetric topology cryptography*. Entropy, 25(5):720, 2023. https://doi.org/10.3390/e25050720.