ANALES DE LA
Academia de Ciencias de Cuba

SECCIÓN CIENCIAS NATURALES Y EXACTAS

Artículo original de investigación

Avances en la caracterización de los códigos lineales y en el criptoanálisis a cifrados en bloque

Mijail Borges Quintana [1*] https://orcid.org/0000-0002-5656-0037
Miguel Angel Borges Trenard [2] https://orcid.org/0000-0001-7154-7730
Edgar Martínez Moro [3] https://orcid.org/0000-0003-1243-2049
Osmani Tito Corrioso [4] https://orcid.org/0000-0003-4231-7674

[1] *Facultad de Ciencias Naturales y Exactas, Universidad de Oriente. Santiago de Cuba, Cuba*
[2] *Universidad Antonio Nariño. Bogotá, Colombia*
[3] *Instituto de Matemática, Universidad de Valladolid. Valladolid, España*
[4] *Centro Universitario Municipal Cárdenas, Universidad de Matanzas. Matanzas, Cuba*

[*] *Autor para la correspondencia:* mijail@uo.edu.cu

Editor

Lisset González Navarro
Academia de Ciencias de Cuba.
La Habana, Cuba

Traductor

Darwin A. Arduengo García
Academia de Ciencias de Cuba.
La Habana, Cuba

RESUMEN

Introducción: Se aborda el problema de la necesidad de diseñar metodologías que contribuyan a la caracterización de la estructura combinatoria de los códigos lineales y de grupo, y al proceso del criptoanálisis de cifrados en bloques. **Objetivo:** Caracterizar conjuntos esenciales de un gran tamaño que permitan elaborar metodologías para procesos que intervienen en estructuras asociadas con los líderes de cosetos de los códigos lineales y el conjunto de claves de los cifrados en bloques. **Métodos:** Los algoritmos que se elaboran a partir de las metodologías diseñadas, si bien construyen una lista de objetos de un tamaño considerable, se logra que los mismos generen una cantidad de elementos cercana al tamaño de los conjuntos que se desean construir. Se caracterizan matemáticamente estructuras algebraicas esenciales, se formulan y demuestra la corrección de algoritmos para el cálculo de las estructuras, se realizan instrumentación de los algoritmos en sistemas de Algebra Computacional (Maple y GAP), se desarrollan experimentaciones y se realizan comparaciones y conjeturas a partir de los patrones observados. **Resultados:** Los resultados específicos se pueden agrupar en 2 direcciones, la caracterización y construcción de las palabras líderes de un código lineal, y el diseño de metodologías de ataque a cifrados en bloques y caracterización de estructuras algebraicas con aplicaciones en la criptografía. **Conclusiones:** Para la caracterización y elaboración de las metodologías propuestas ha sido esencial la combinación de un estudio algebraico con el diseño de algoritmos y prueba de implementaciones con los objetos bajo estudio.

Palabras clave: códigos lineales; líderes de cosetos; palabras líderes; criptoanálisis; cifrados en bloque

Premio Nacional Anual de la Academia de Ciencias de Cuba, 2023

Advances in the characterization of linear codes and in the cryptanalysis of block ciphers

ABSTRACT

Introduction: There is a need of methodologies that contribute to the characterization of the combinatorial structure of linear and group codes, and to the process of cryptanalysis of block ciphers. **Objective:** To characterize large essential sets that allow the development of methodologies for processes involving structures associated with the coset leaders of linear codes and the set of keys of block ciphers. **Methods:** The algorithms developed from the designed methodologies, while constructing a list of objects of considerable size, manage to generate a number of elements close to the size of the sets to be constructed. Essential algebraic structures are mathematically characterized, the correctness of algorithms for computing the structures is formulated and demonstrated, the algorithms are built in Computer Algebra systems (Maple and GAP), experiments are carried out, and comparisons and conjectures are made based on the observed patterns. **Results:** The characterization and construction of the leader codewords of a linear code, and the design of attack methodologies for block ciphers and the characterization of algebraic structures with applications in cryptography. **Conclusions:** The combination of an algebraic study with the design of algorithms and implementation testing on the objects under study has been essential for the characterization and development of the proposed methodologies.

Keywords: linear codes; coset leaders; leader codewords; cryptanalysis; block ciphers

INTRODUCCIÓN

La teoría de códigos y la criptografía constituyen 2 campos muy importantes en las telecomunicaciones y los procesos de informatización de la sociedad. Los mismos constituyen fuentes indispensables de protocolos, medios y herramientas que garantizan el proceso de transmisión de la información de forma estable y segura, jugando un papel esencial en las comunicaciones. Al mismo tiempo, la teoría de códigos es una herramienta fundamental para garantizar la integridad en la transmisión de los textos criptográficos cifrados, permitiendo la detección y corrección de errores. En este contexto la disciplina de Álgebra computacional interviene tanto en el desarrollo de fundamentaciones teóricas de estructuras y métodos que se utilizan en estos procesos, como también en la formulación e implementación de protocolos, metodologías y procedimientos.

En este trabajo se aborda el problema de la necesidad de diseñar metodologías que contribuyan a la caracterización de la estructura combinatoria de los códigos lineales y de grupo, y al proceso del criptoanálisis de cifrados en bloques, para ello se estudian 2 conjuntos de gran tamaño que tienen una gran incidencia en problemas vinculados con la teoría de códigos y la criptografía, y en la generalidad de los casos son imposibles de recorrer completamente. Estos objetos son el conjunto de líderes de cosetos de un código lineal y el conjunto de las claves de un cifrado en bloque. [1,2] En ambos casos las investigaciones se dirigen hacia la caracterización de los objetos que permitan el diseño de metodologías basadas en dichas estructuras, de modo que se obtengan mejores propiedades de dichos conjuntos y a la vez sea más fácil su tratamiento.

Los líderes de cosetos están vinculados con muchos problemas combinatorios de gran importancia para los códigos lineales, tales como: el cálculo del radio de Newton, el radio de cobertura y el cálculo de la distribución de pesos de los líderes de cosetos, el cual es un problema que permanece no resuelto para muchas familias de códigos lineales. El estudio del conjunto de los líderes de cosetos es también clave en la caracterización de los errores corregibles y no corregibles de un código lineal y para el diseño de algoritmos de decodificación por distancia mínima, así como para la construcción de palabras del código de soporte mínimo las cuales juegan un papel muy importante para el diseño de esquemas de compartimiento de secretos y la construcción de invariantes para la determinación de la equivalencia de códigos, mediante el diseño de algoritmos que utilizan los invariantes para la construcción de firmas. [3] Estas aplicaciones

en el diseño de esquemas de compartimiento de secretos y la equivalencia de códigos vinculan la primera dirección de la investigación, en el contexto de la teoría de códigos, con la segunda vinculada con la criptografía.

En el campo de la criptografía se investigan los cifrados en bloque, en particular, el estudio y diseño de métodos de criptoanálisis, o sea métodos de ataques contra estos sistemas criptográficos. [2] Lo cual implica trabajar con el conjunto de las claves de dichos cifrados.

Los objetivos del trabajo fueron ccaracterizar el conjunto de los líderes de cosetos de los códigos lineales y códigos de grupo y diseñar herramientas algebraicas y metaheurísticas para la utilización de diversos métodos de criptoanálisis a los cifrados en bloques.

MÉTODOS

Las investigaciones correspondientes a este trabajo tienen un carácter esencialmente básico, aborda el problema sobre el diseño de metodologías que contribuyan a la caracterización de la estructura combinatoria de los códigos lineales y de grupo, y al proceso del criptoanálisis de cifrados en bloques. No obstante, las caracterizaciones de los objetos y estructuras algebraicas pueden ser útiles en estudios para aplicaciones en el contexto de las telecomunicaciones, en el proceso de codificación y seguridad en la transmisión y procesamiento de información. Los estudios que han tributado a los resultados han sido coordinados por el Grupo de álgebra computacional y criptografía de la Universidad de Oriente por un período del 2008 al 2023 con particular énfasis en los últimos 5 años.

El ideal asociado a un código lineal ofrece la posibilidad de utilizar las bases de Gröbner de estos ideales para problemas vinculados con los códigos, como la decodificación y la determinación de la equivalencia de códigos. [4] Las bases de Gröbner asociadas a los códigos lineales y la definición y algoritmo de cálculo de las mismas y las representaciones de Gröbner de los códigos lineales. Ese resultado constituye punto de partida esencial para el cumplimiento del primer objetivo de este trabajo. Se muestra otra forma de introducir el ideal asociado al código para un código binario y se muestran propiedades que relacionan cierto conjunto de palabras del código con las bases de Gröbner asociadas a sus ideales, estas palabras se denominaron palabras de Gröbner y constituyen la base para la definición y construcción de las palabras líderes.

Tomando el trabajo de Borges-Quintana *et al*. como punto de partida, Márquez-Cobella introduce esta forma de asociar el ideal con un código lineal cualquiera, permitiendo como en el caso binario el cálculo de sus bases de Gröbner compatibles con el proceso de decodificación. [5,6] Por otra parte, Aliasgari generaliza los ideales asociados a códigos para la construcción de ideales asociados a látices. [7] Posteriormente, los autores Álvarez-Barrientos *et al.* muestran 3 formas equivalentes de construir los ideales asociados a látices generalizando el estudio de las propiedades combinatorias de los códigos binarios teniendo en cuenta estructuras relacionadas con sus bases de Gröbner asociadas, además se formula un algoritmo tipo Möller para el cálculo de las bases de Gröbner asociadas con estos ideales. [8,9]

De ahí que, en el contexto de los códigos lineales, y más general, códigos de grupos, en el presente trabajo se avanza en 2 direcciones, por una parte, en la caracterización de estructuras muy vinculadas con los líderes de cosetos, como lo son las palabras de Gröbner y las palabras líderes, así como la caracterización de algunas propiedades combinatorias de las mismas y aplicaciones, como la decodificación de códigos y la determinación de la equivalencia de los mismos. Por otra parte, se avanza en la formulación y fundamentación de algoritmos tipo Möller para el cálculo de estas estructuras.

Por otro lado, el criptoanálisis algebraico (CA) es el proceso de romper códigos mediante la resolución de sistemas de ecuaciones polinómicos. Algunos métodos de ataque a cifrados en bloques han mostrado ser potencialmente útiles. Se realizan combinaciones de ataques como el lineal y diferencial, mezcladas también con técnicas heurísticas, para buscar una cierta automatización del proceso. [10]

Hay varios métodos y herramientas que son utilizados como métodos de optimización y predicción. Varios algoritmos heurísticos han sido empleados en el contexto de la Criptografía, tales como el algoritmo colonia de hormigas (ACO), el algoritmo de búsqueda tabú y el algoritmo genético, entre otros.

En este contexto de la Criptografía los conjuntos de gran tamaño que se estudian en el trabajo son el conjunto de claves privadas de los cifrados en bloques, del tamaño de este conjunto depende en gran medida la seguridad de los cifrados en bloques correspondientes. En este sentido, teniendo en cuenta las diferentes tendencias de criptoanálisis a los cifrados en bloque se proponen varias metodologías de ataque.

RESULTADOS

Desarrollo de un algoritmo de tipo Möller para el cálculo de representaciones de Gröbner de ideales asociados a códigos de grupo

Caracterización de las palabras líderes de códigos lineales

Las bases de Gröbner para códigos lineales fueron introducidas en la tesis doctoral de Borges-Quintana, posteriormente Borges-Quintana *et al*. introducen el ideal asociado al

código y se formula y fundamenta un algoritmo para el cálculo de las bases de Gröbner asociadas a códigos lineales. [4] También se ha mostrado otra forma de obtener el ideal asociado al código la cual está directamente vinculada a la construcción de binomios asociados con las palabras del código que conforman un conjunto generador y así ofrece la posibilidad de asociar una base de Gröbner del código con la base de Gröbner del ideal generado por estos binomios. [5]

Mora *et al*. analizan los avances en las interconexiones entre las bases de Gröbner, la teoría de códigos y la criptografía. [11] En este trabajo se realiza una formalización general de los algoritmos tipo Möller por uno de sus desarrolladores principales, se muestra la formulación del algoritmo tipo Möller para los códigos lineales y su repercusión en la caracterización de varias propiedades asociadas con los códigos. [9,12] Esto resulta importante en la construcción de invariantes para los códigos lo cual tiene aplicaciones en múltiples problemas combinatorios, la identificación de familias de códigos, la equivalencia de códigos y la construcción de estructuras para el diseño de esquemas de compartimiento de secretos.

Se extiende el concepto de representación de Gröbner a matroides binarias. [13] Por otra parte, se utiliza la estructura de la representación de Gröbner del ideal asociado a los códigos de evaluaciones para calcular el número de elementos de la firma de ese ideal, lo cual permite determinar parámetros del código como la dimensión. [14]

Las representaciones de Gröbner calculan un representante de cada clase de equivalencia que determina el código y una forma de operar entre clases de equivalencia que permite entre otras cosas determinar a qué clase pertenece cada palabra, el conjunto de representantes de la representación de Gröbner se extiende al cálculo del conjunto de los líderes de cosetos y se introducen las palabras de Gröbner como conjunto de palabras del código con buenas propiedades combinatorias relacionadas con el código. [15] El conjunto de palabras de Gröbner constituye un *trial set* para códigos binarios. [16]

Asociado al conjunto de los líderes de cosetos se define una estructura para cualquier código lineal denominada el ideal débil ordenado asociado al código lineal, se muestra cómo ésta es una estructura de tamaño mínimo que debe generar un algoritmo para el cálculo de los líderes de cosetos. [17] Se extiende el concepto de palabras líderes de códigos binarios a cualquier código lineal, y se muestra cómo pueden caracterizarse en función de ello el conjunto de los errores corregibles y no corregibles del código.

La estructura del ideal débil ordenado permite fundamentar un algoritmo para el cálculo de las palabras líderes asociadas a cualquier código lineal, generando un mínimo número de elementos de acuerdo al tamaño del conjunto que se quiere obtener, por otra parte, es posible calcular el conjunto de las palabras líderes por niveles de acuerdo a su peso, incluso detener el cálculo de acuerdo a la cantidad de niveles deseado, permitiendo el correspondiente ahorro de tiempo de cómputo y espacio de memoria. [18]

Siguiendo la construcción de los ideales asociados a códigos de látices, lo cual está basado en la asociación que se hace en investigaciones precedentes para códigos binarios, se formalizan 3 formas de obtener el ideal asociado a cualquier código de grupo, en particular a los códigos de látices. [7,5,8] Se fundamenta además un algoritmo tipo Möller para el cálculo de las bases de Gröbner asociadas con los códigos de látices. Borges-Quintana y Ornella-Rodríguez [19] definen un tipo de base de Gröbner, denominada base completa de códigos lineales, las cuales constituyen bases de Gröbner para cualquier orden de grado total, por lo que resulta un objeto vinculado estrechamente con cada código lineal. Además, se formula y fundamenta un algoritmo tipo Möller para su cálculo, donde nuevamente el ideal débil ordenado del código es muy importante.

Diseño de metodologías de ataque a cifrados en bloque con la combinación de herramientas evolutivas y algebraicas

El estudio de técnicas modernas de criptoanálisis a cifrados en bloque con parámetros moderados comienza con Moreno-Ramírez *et al*., en este caso es de destacar el estudio del método Time Memory Trade Off (TMTO) para invertir funciones de una sola vía. [20] El propósito del TMTO es invertir funciones de sentido único, empleando para ello un tiempo menor al de una búsqueda exhaustiva y una memoria inferior a la utilizada en una tabla de correspondencia. [21]

Los cifrados en bloques son funciones de una sola vía y la principal complejidad para ello viene dada en el objeto bajo estudio en este campo, el conjunto de las claves posibles, el cual es un conjunto de gran tamaño en relación con los parámetros de los cifrados. Se trata de que para un cifrado en bloque es relativamente fácil calcular el cifrado de un texto claro, pero es "difícil" calcular el texto claro a partir de su cifrado. Se propone un método de optimización lineal para seleccionar los parámetros del TMTO, las restricciones del modelo están dirigidas a obtener condiciones admisibles del modelo para un tiempo y memoria máxima dada. [20] Los experimentos confirman que el esquema propuesto determina los parámetros con el objetivo de descifrar el mensaje con una alta probabilidad, o sea invertir la función del cifrado en bloque.

En relación al criptoanálisis algebraico, también se utilizan las bases de Gröbner como método de solución de los

sistemas de ecuaciones polinómicos. Proponiendo metodologías para la aplicación de estos ataques a cifrados en bloque y creando herramientas algorítmicas y computaciones para el perfeccionamiento de los métodos. [22]

En esta dirección se realiza un estudio de varios representantes de la denominada familia de cifrados en bloques ligeros. [23] Se realiza un análisis detallado de los algoritmos de generación de claves, de cifrado y descifrado, así como una programación de estos algoritmos en el sistema de cálculo simbólico MAPLE, además, se hacen comparaciones entre los cifrados y entre sus implementaciones. Se estudian los métodos de modelación de primitivas de los cifrados y de criptoanálisis algebraico. Se aplica el ataque algebraico sobre seis rondas de los cifrados SIMON y SIMECK, logrando recuperar los 64 bits de la clave en ambos casos. Se logró el modelado simbólico de las operaciones del cifrado PRINT, incluyendo su permutación dependiente de la clave y se le aplicó también el criptoanálisis algebraico. Se presenta una alternativa al ataque algebraico utilizando "Sat-solvers", la cual emerge de la utilización de técnicas de las bases de Gröbner y las potencialidades para la solución de los sistemas de ecuaciones polinómicas que tiene el sistema de álgebra computacional MAPLE.

Otra tendencia en las técnicas de criptoanálisis es la utilización de métodos heurísticos. Existen varios de ellos y otras herramientas que son utilizados como métodos de optimización y predicción. Varios algoritmos heurísticos han sido empleados en el contexto de la Criptografía. El algoritmo genético (AG) es un método de optimización utilizado en los últimos años en la Criptografía con diversos propósitos, en particular con el de realizar ataques a varios tipos de cifrados.

Buscar la clave en todo el espacio de las claves es un problema y puede llegar a ser imposible en la práctica debido al gran tamaño del conjunto de las claves. En este sentido, se diseñan 2 metodologías de partición del espacio de claves que utilizan el algoritmo de la división con resto, la metodología BBM que en esencia fija un cierto número de componentes de la clave al inicio del bloque, y la metodología TBB, que mantiene fijas las componentes correspondientes a un mismo resto que representa una de las clases de equivalencia que determina el algoritmo de la división con resto. [24,25]

Con estas 2 metodologías de particionamiento del conjunto de claves se determina cómo hacer un balance entre la cantidad de clases de equivalencia y la cantidad de elementos dentro de éstas, y cómo obtener información sobre la clase que contiene o puede contener la clave. [25] Por otro lado, se realiza el estudio de ciertas variantes y parámetros relacionados con el AG, como el tiempo que demora para ejecutar un determinado número de iteraciones, de manera que se pueda estimar una cantidad de generaciones a realizar en un tiempo disponible, de acuerdo con ello se puede escoger el tamaño del conjunto de individuos que constituyen soluciones admisibles para el AG; se introducen otras funciones de aptitud y se analiza cuáles son las que conducen a mejores resultados. Se propone un método de ataque con el cual es posible desechar algunas clases, reduciendo el número total que sería necesario recorrer; en conexión con esta propuesta, se obtienen condiciones necesarias y fórmulas para estimar los valores de los parámetros que determinan un balance entre el número de clases en que se divide el espacio de las claves y el número de elementos dentro de cada una de ellas, resolviendo el problema de la elección óptima de estos parámetros. [26]

Además, se propone una metodología con la que se comprueba que la cercanía a 1 del valor de algunas funciones de aptitud que emplean distancia decimal, implica cercanía decimal a la clave. Y se inicia la base de una teoría que permita caracterizar las funciones de aptitud y determinar, *a priori*, si una es más efectiva que otra en el ataque a cifrados en bloque mediante el AG. [27]

Se propuso otra metodología para particionar el espacio de las claves, la cual constituye un método de reducción sucesiva del conjunto de las posibles soluciones mediante el procedimiento de fijar componentes de la clave iterativamente. Con esta herramienta se muestran los resultados del criptoanálisis realizado al cifrado PRESENT-80. [28]

La idea en el criptoanálisis algebraico, de transformar el cifrado en un sistema de ecuaciones, se puede realizar de diferentes formas, en particular, utilizando sistemas de ecuaciones del tipo MRHS (multiple right hand side), una forma especial para transformar los cifrados en bloque. La particularidad principal de estos sistemas es que el término independiente no es único para cada ecuación, sino, que es un conjunto de términos independientes. En ese sentido, se propone el uso del AG, como método de solución de estos sistemas de ecuaciones; además, se proponen 3 funciones de aptitud que permiten conectar los sistemas MRHS con el AG. [29]

DISCUSIÓN

El estudio de propiedades combinatorias de los códigos lineales y su comportamiento en familias de códigos continúa siendo un problema de interés y de mucha importancia en esta disciplina. Se han estudiado las palabras de mínimo peso de códigos lineales ternarios y una cota inferior de la distancia mínima de estos códigos. [30] Mientras que la distribución de pesos de las palabras del código, las palabras de un mismo peso y su soporte en familias de códigos cíclicos. [31]

Las palabras líderes asociadas con los códigos lineales tienen mucha relación desde el punto de vista algebraico con las bases de Gröbner asociadas a los códigos lineales, lo cual

permite que estudiando estas estructuras y caracterizándolas se pueda mejorar la potencialidad algorítmica en la solución de problemas complejos. Desde el punto de vista combinatorio las palabras líderes tienen mucha relación con la estructura de líderes de cosetos de los códigos lineales.

Una muestra de la actualidad de investigaciones relacionadas con los líderes de cosetos lo constituyen, por ejemplo, los trabajos de Yan *et al*. donde se estudian los cosetos ciclotómicos de una familia de códigos LCD BCH, y Huang *et al*. con la utilización del estudio de las propiedades de los líderes de cosetos para la construcción de ciertos códigos LCD BCH y se determinan sus parámetros; además, se muestran las potencialidades de este estudio para aplicaciones en implementaciones criptográficas que impidan ataques tipo canal colateral, evidenciando que el estudio de estas estructuras de los códigos lineales puede conllevar a aplicaciones en el campo de la Criptografía. [32,33] Lo cual ha sido también una dirección de este trabajo mediante la utilización de las estructuras invariantes obtenidas en la propuesta de algoritmos y procedimientos para la determinación de la equivalencia de códigos. [17,18,19]

A pesar del carácter abstracto y más teórico de este tipo de investigaciones en la teoría de códigos, Liu *et al*. muestran que pueden ser de gran importancia en el desarrollo de un esquema de decodificación por líderes de cosetos para un tipo de nueva generación de memoria RAM. [34] Como ya se ha descrito anteriormente el estudio de las palabras líderes, conjuntos *test set* y bases completas de los códigos lineales permiten la construcción de invariantes. Al respecto, en varios trabajos se ha estudiado la cápsula de ciertos códigos lineales como estructuras invariantes, y los parámetros invariantes de la familia de códigos BCH como la distancia mínima y la dimensión, así como la relación de este estudio con la estructura de los líderes de cosetos. [35,36]

Con respecto al campo de la criptografía cada vez resulta de mayor importancia el desarrollo de nuevas metodologías de ataques con la combinación de varios enfoques y técnicas algebraicas y heurísticas. Por una parte, este proceso logra poner a prueba la seguridad de los protocolos que se establezcan para ciertos fines y desarrollar otros nuevos. Por otra parte, contribuyen al desarrollo de nuevos conocimientos en este campo en la frontera de la Matemática, Ciencia de la Computación, Informática y las Telecomunicaciones. Se observa la vigencia de la utilización de métodos de Criptoanálisis no heurísticos. [37]

Biyashev *et al*. proponen una metodología de CA basada en una linealización del sistema de ecuaciones algebraicas que modela el cifrado, teniendo en cuenta para ello las S-cajas que constituyen el comportamiento no lineal del cifrado en bloque. [37,22,23]

Por otro lado, el campo de la Criptografía Ligera es relativamente nuevo, su esencia consiste en la necesidad de encontrar compromisos entre ligereza y seguridad, lo cual es una demanda del desarrollo actual, en el cual se cuenta con dispositivos y plataformas de diversa índole; no sólo computadoras tradicionales que requieren protección criptográfica; además de la era de "Internet en las Cosas", la cual permite que los objetos sean detectados y controlados remotamente, a través de la infraestructura de red existente. Los cifrados en bloque ligeros, vulnerabilidades y métodos de criptoanálisis son analizados por Labrada-Claro *et al*. [23]

En relación a la utilización de los métodos heurísticos en el criptoanálisis tienen una aplicación cada vez mayor, incrementando sus potencialidades en la medida que la tecnología se desarrolla, la cual exige a su vez la actualización de los parámetros de seguridad de los protocolos criptográficos y el diseño de otros nuevos. En esencia el problema de llevar a cabo algún método de Criptoanálisis está relacionado con el intento de resolver problemas de naturaleza muy compleja, los cuales resultan muy difíciles de resolver por métodos exactos y determinísticos. Es por ello que surge la necesidad creciente del uso de las herramientas heurísticas, teniendo en cuenta la teoría relacionada con la construcción de los cifrados.

El AG resulta uno de los métodos heurísticos más utilizados por la comunidad científica en la criptografía. Grari *et al*. utilizan el método heurístico de colonia de hormigas (ACO por sus siglas en inglés "ant colony optimization") y se prueba una metodología con el S-AES (Simplified Advanced Encryption Standard), se trabaja con 2 pares de textos planos y textos cifrados. Hassan *et al*., utilizan una combinación de los métodos AG y ACO para el criptoanálisis de cifrados en flujo. Por otra parte, Pavlenko *et al*. trabajan con la combinación de 2 algoritmos evolutivos, el (1+1)-EA y el AG, en conjunto con el de búsqueda tabú, en este caso estos algoritmos utilizan estrategias basadas en los llamados SAT-solvers (solución del problema de satisfacibilidad booleana) y se comprueban las metodologías propuestas con varios cifrados en flujo. [38,39,40]

Los resultados del presente trabajo comprenden la caracterización de las palabras líderes y las bases de Gröbner de códigos lineales, su relación con los conjuntos *test set* y la construcción de invariantes de los códigos. Se incluye la formulación de algoritmos eficientes tipo Möller para el cálculo de las estructuras y la implementación de las mismas para el desarrollo de experimentaciones.

Se investigan y desarrollan varios métodos de ataque a cifrados en bloque como el ataque algebraico y ataque por algoritmo genético, con respecto a este último se realizan estudios del comportamiento de varios de sus parámetros, así como el diseño de una metodología de particionamiento del

espacio de llaves. Se elaboran las herramientas computacionales necesarias para la experimentación.

Las estructuras de las palabras líderes, los *trial set*, las bases completas y las vinculadas a las matroides binarias y los látices tienen gran significación para el campo de la criptografía, en particular la denominada criptografía postcuántica. [15,17,16,19,13,8] El estudio y profundización en las mismas representa potenciales aplicaciones en este otro campo, resultando ésta una conexión entre los resultados 1 y 2 en el campo de la teoría de códigos y el resultado 3 en el campo de la criptografía. Este enlace alcanza su mayor concreción en el trabajo con el diseño de una firma, a partir del conjunto de las palabras líderes, en la formulación y fundamentación de un algoritmo para la determinación de la equivalencia de códigos. [3,18]

Conclusiones

En este trabajo se ha logrado introducir nuevas estructuras algebraicas relacionadas con propiedades combinatorias esenciales de los códigos lineales y aplicar la utilización de estas estructuras en el desarrollo de metodologías y herramientas computacionales para los procesos de decodificación, caracterización de la estructura de los líderes de cosetos (errores corregibles y no corregibles), construcción de estructuras invariantes y utilización de las mismas para la determinación de la equivalencia de códigos, lo cual tiene también repercusión en el campo de la criptografía.

Las bases de Gröbner y estructuras similares han sido utilizadas tanto con una asociación directa a objetos de los códigos lineales como también han resultado una herramienta algebraica utilizada para el procesamiento algebraico de modelos polinomiales con un fin determinado, para los cuales incluso la selección o construcción de un ordenamiento adecuado resulta clave. En esa dirección, este procedimiento fue aplicado tanto en aplicaciones a la teoría de códigos como a la criptografía. De esta forma, las bases de Gröbner constituyen uno de los puntos principales de conexión en el trabajo entre las investigaciones realizadas para resolver los problemas propuestos.

Las investigaciones desarrolladas en el campo de la criptografía han requerido del análisis de métodos algebraicos y heurísticos, y del desarrollo de herramientas computacionales para la experimentación. Este análisis conjunto ha permitido desarrollar metodologías de ataque a cifrados en bloques y realizar determinadas propuestas para un mejor funcionamiento de estos ataques. En particular, en el caso del Algoritmo Genético se ha propuesto un procedimiento de particionamiento de llaves y se han mostrado sus potencialidades en el proceso de cómputo.

REFERENCIAS BIBLIOGRÁFICAS

1. Huffman WC, Pless V. Fundamentals of error-correcting codes. Cambridge, England (United Kingdom): Cambridge University Press; 2003.
2. Menezes A, van Oorschot P, Vanstone S. Handbook of Applied Cryptography. CRC Press; 1996.
3. Sendier N. Finding the Permutation Between Equivalent Linear Codes: The Support Splitting Algorithm. IEEE Trans. Inform. Theory. 2000;46(4):1193-203.
4. Borges-Quintana M, Borges-Trenard MA, Martínez-Moro E. On a Gröbner bases structure associated to linear codes. J. Discrete Math. Sci. Cryptogr. 2007;10(2):151-91.
5. Borges-Quintana M, Borges-Trenard MA, Martínez-Moro E. Gröbner basis and combinatorics for binary codes. Appl. Algebra Engrg. Comm. Comput. 2008;19(5):393-411.
6. Márquez-Cobella I. A Combinatorial Commutative Algebra Approach to Complete Decoding [tesis doctoral]. Valladolid (España): Universidad de Valladolid; 2013.
7. Aliasgari M, Sadeghi MR, Panario D. Gröbner bases for lattices and an algebraic decoding algorithm. IEEE Trans. on Communications. 2013;61(4):1222-30.
8. Álvarez-Barrientos I, Borges-Quintana M, Borges Trenard MA, Panario D. Computing Gröbner bases associated with lattices. Adv. Math. Commun. 2016; 10(4): 853-62.
9. Mora T. The FGLM problem and Möller's algorithm on zero-dimensional ideals. Gröbner, Coding, and Cryptography. Springer. 2009:379-84.
10. Dobraunig CE, Eichlseder M, Mendel F. Heuristic Tool for Linear Cryptanalysis with Applications to CAESAR Candidates. In: Advances in Cryptology-ASIACRYPT 2015. LNCS;9453. Springer; 2015. Disponible en: https://doi.org/10.1007/978- 3-662-48800-3_20
11. Mora T, Perret L, Sakata S, Sala M, Traverso C, editors. Gröbner, Coding, and Cryptography. Linz (Austria): RISC Book Series, Springer; 2009. Disponible en: https://doi.org/10.1007/978-3-540-93806-4
12. Borges-Quintana M, Borges-Trenard MA, Martínez-Moro E. An application of Möller's Algorithm to Coding Theory. In: Mora T, Perret L, Sakata S, Sala M, Traverso C, editors. Gröbner, Coding, and Cryptography. Linz (Austria): RISC Book Series, Springer, 2009;379-84. Disponible en: https://doi.org/10.1007/978-3-540-93806-4_24
13. Borges-Quintana M, Borges-Trenard MA, Martínez-Moro E. Gröbner representation of binary matroids. Paper presented at: Bras-Amarós M, Høholdt T, editors. Proceedings of Applied algebra, Algebraic algorithms, and Error Correcting Codes (AAECC'09), Lecture Notes in Comput. Sci. 2009; 5527: 227-30.
14. Borges-Quintana M, Borges-Trenard MA, Galindo C. Improved Evaluation Codes Defined by Plane Valuations. Finite Fields Appl. 2010;16:265-76.
15. Borges-Quintana M, Borges-Trenard MA, Márquez-Corbella I, Martínez-Moro E. Computing coset leaders and leader codewords of binary codes. J. Algebra Appl. 2015;14(8):1-19.
16. Borges-Quintana M, Borges-Trenard MA, Martínez-Moro E. Trial set and Gröbner bases for binary codes. Applications of Computer Algebra "ACA 2015". Springer Proc. Math. Stat. 2017;198:21-7. Disponible en: https://doi.org/10.1007/978-3-319- 56932-1_3
17. Borges-Quintana M, Borges-Ternard MA, Martínez-Moro E. On the Weak Order Ideal Associated to Linear Codes. Math. Comput.

Sci. 2018;12:339-47. Disponible en: https://doi.org/10.1007/s11786-018-0349-1
18. Borges-Quintana M, Borges-Trenard MA, Martínez-Moro E, Torres-Guerrero G. Computing an Invariant of a Linear Code. In: Slamanig D, Tsigaridas E, Zafeirakopoulos Z, editors. Mathematical Aspects of Computer and Information Sciences (MACIS 2019). Lecture Notes in Comput. Sci., Springer. 2020;11989:218-33.
19. Borges-Quintana M, Ornella-Rodríguez JA. Cálculo de bases de Gröbner completas asociadas a códigos lineales. Ciencias Matemáticas. 2019;33(1):28-35.
20. Moreno-Ramírez J, Borges-Quintana M, Borges-Trenard MA. Choosing TMTO Parameters by means of Linear Optimization. IEEE América Latina. 2015;13(8):2723-27.
21. Mukhopadhyay S. A Study on Time/Memory Trade-Off Cryptanalysis [doctoral thesis]. India: Indian Statistical Institute; 2006.
22. Martínez-Ferrer I, Borges Trenard MA, Borges Quintana M. Criptoanálisis algebraico a cifrados en bloques. Ciencias Matemáticas. 2019;33(1):36-45.
23. Labrada-Claro R, Borges-Trenard MA, Borges-Quintana M. Criptoanálisis algebraico a los cifrados en bloques ligeros SIMON y SIMECK. Revista Cubana de Ciencias Informáticas. 2023;17(1):53-66.
24. Borges-Trenard MA, Borges-Quintana M, Monier-Columbié L. An application of genetic algorithm to cryptanalysis of block ciphers by partitioning the key space. J. Discrete Math. Sci. Cryptogr. 2019. Disponible en: https://doi.org/10.1080/09720529.2019.1649028
25. Tito-Corrioso O, Borges-Trenard MA, Borges-Quintana M, Rojas O, Sosa-Gómez G. Study of Parameters in the Genetic Algorithm for the Attack on Block Ciphers. Symmetry. 2021;13(806):1-12. Disponible en: https://doi.org/10.3390/sym13050806
26. Tito-Corrioso O, Borges-Quintana M, Borges-Trenard MA. Attack to block ciphers by class elimination using the Genetic Algorithm. Revista Investigación Operacional. 2023;44(2):249-63.
27. Tito-Corrioso O, Borges-Quintana M, Borges-Trenard MA, Rojas O, Sosa-Gómez G. On the Fitness Functions Involved in Genetic Algorithms and the Cryptanalysis of Block Ciphers. Entropy. 2023;25(261):1-13. https://doi.org/10.3390/e25020261
28. Donatién-Charón A, Borges-Trenard MA, Borges-Quintana M. Ataque al PRESENT-80 con el Algoritmo Genético mediante aproximaciones sucesivas de componentes fijas. Revista Cubana de Ciencias Informáticas. 2023;17(1):1-15.
29. Tito-Corrioso O, Borges-Quintana M, Borges-Trenard MA. Improving search of solutions of MRHS systems using the Genetic Algorithm. Revista Cubana de Ciencias Informáticas. 2023;17(1):38-52.
30. Ding C, Tang C, Tonchev VD. Linear codes of 2-designs associated with subcodes of the ternary generalized Reed–Müller codes. Des. Codes Cryptogr. 2020; 88: 625- 41.
31. Du X, Wang R, Fan C. Infinite families of 2-designs from a class of cyclic codes. J Combin. Designs. 2020;28:157-70.
32. Yan H, Liu H, Li Ch, Yang Sh. Parameters of lcd bch codes with two lengths. Adv. Math. Commun. 2018;12(3):579-94.
33. Huang X, Yue Q, Wu Y. Binary primitive LCD BCH codes. Des. Codes Cryptogr. 2020;88:2453-73.
34. Liu L, Zhuang Y, Zhang L, Tang H, Dong S. Proactive correction coset decoding scheme based on SEC-DED code for multibit asymmetric errors in STT-MRAM. Microelectronics Journal. 2018;82:92-100.
35. Liu H, Pan X. Galois hulls of linear codes over finite fields. Des. Codes Cryptogr. 2020;88:241-55.
36. Liu Y, Li R, Fu Q, Lu L, Rao Y. Some binary BCH codes with length n = 2m + 1. Finite Fields Appl. 2019;55:109-33.
37. Biyashev R, Dyusenbayev D, Algazy K, Kapalova N. Algebraic Cryptanalysis of Block Ciphers. Proceedings of the 2019 International Conference on Wireless Communication, Network and Multimedia Engineering (WCNME 2019). Atlantis Press; 2019. p. 129-32.
38. Grari H, Azouaoui A, Zine-Dine K. A cryptanalytic attack of simplified-AES using ant colony optimization. International Journal of Electrical and Computer Engineering. 2019;9(5):4287-95.
39. Hassan F, Riyam A, Jawad N. Using Evolving Algorithms to Cryptanalysis Nonlinear Cryptosystems. Baghdad Science Journal. 2020;17(2).
40. Pavlenko A, Semenov A, Ulyantsev V. Evolutionary Computation Techniques for Constructing SAT-Based Attacks in Algebraic Cryptanalysis. In: Kaufmann P, Castillo P, editors. Applications of Evolutionary Computation. EvoApplications 2019. Lecture Notes in Comput. Sci. Vol. 11454. Springer; 2019.

Recibido: 24/06/2025
Aprobado:6/06/2025

Agradecimientos

Los autores agradecen a los colaboradores nacionales e internacionales por su contribución a este resultado científico: Ismara Álvarez Barrientos, Adrian Donatien Charón, Jorge Reynaldo Moreno Ramírez, José Ángel Ornella Rodríguez, Gustavo Torres Guerrero, Irene Martínez Ferrer, Roberto Labrada Claro, Lázaro Monier Columbié, Guillermo Sosa, Omar Rojas, Daniel Panario, Irene Márquez-Corbella, Carlos Galindo, Patrick Fitzpatrick, Cristina Gracías-González.

Conflictos de intereses

Los autores declaran no poseer conflictos de intereses en relación con la investigación.

Contribuciones de los autores

- Conceptualización: Mijail Borges Quintana, Miguel Ángel Borges Trenard
- Curación de datos: Mijail Borges Quintana, Miguel Ángel Borges Trenard, Osmani Tito Corrioso
- Análisis formal: Mijail Borges Quintana, Miguel Ángel Borges Trenard
- Adquisición de fondos: Mijail Borges Quintana, Miguel Ángel Borges Trenard, Edgar Martínez Moro
- Investigación: Mijail Borges Quintana, Miguel Ángel Borges Trenard, Edgar Martínez Moro, Osmani Tito Corrioso
- Metodología: Mijail Borges Quintana, Miguel Ángel Borges Trenard, Edgar Martínez Moro
- Administración del proyecto: Mijail Borges Quintana
- Recursos: Mijail Borges Quintana, Miguel Ángel Borges Trenard, Edgar Martínez Moro
- Software: Mijail Borges Quintana, Miguel Ángel Borges Trenard, Osmani Tito Corrioso
- Supervisión: Mijail Borges Quintana, Miguel Ángel Borges Trenard, Edgar Martínez Moro
- Validación: Mijail Borges Quintana, Miguel Ángel Borges Tre-

nard, Edgar Martínez Moro
- Visualización: Mijail Borges Quintana
- Redacció-borrador original: Mijail Borges Quintana
- Redacción-revisión y edición: Mijail Borges Quintana, Miguel Ángel Borges Trenard, Edgar Martínez Moro, Osmani Tito Corrioso

Financiamientos

El resultado de investigación que se presenta es fruto de 6 proyectos de investigación nacionales e internacionales que se han realizado entre el 2008 al 2023 con diferentes fuentes y montos de financiación. En estos momentos se participa en una red CYTED y 2 proyectos nacionales asociados a programas como entidad participante, responsable de la línea de investigación de Álgebra Computacional y Criptografía (UO y U. Matanzas): Red cyted "nuevas herramientas criptográficas para la e-comunidad (new crypto tools)", 2022-2025; proyecto asociado al Programa Nacional de Telecomunicaciones e Informatización de la Sociedad. Criptografía aplicada a la Seguridad de las Tecnologías de la Información. Instituto de Criptografía, Universidad de la Habana, 2021-2023; Proyecto asociado al Programa Nacional de Ciencias Básicas y Naturales (PNCBN). Investigaciones matemáticas de la criptográfica moderna para el desarrollo de la Informatización de la Sociedad Cubana. Instituto de Criptografía, Universidad de la Habana, 2021-2023. Borges Quintana desarrolló 2 estancias de investigación postdoctoral: en la Universidad de Valladolid, septiembre 2014-febrero 2015, en el marco del programa Erasmus Mundus Lindo; y octubre-noviembre de 2011 en RISC-Linz "Research Institute for Symbolic Computation", Linz, Austria. Borges Trenard desarrolló una estancia de investigación postdoctoral en la Universidad Jaume I, Castellón, España (febrero-marzo de 2009).

Cómo citar este artículo

Borges Quintana M, Borges Trenard MA, Martínez Moro E, Tito Corrioso O. Avances en la caracterización de los códigos lineales y en el criptoanálisis a cifrados en bloque. An Acad Cienc Cuba [Internet] 2025 [citado en día, mes y año];15(2):e3110. Disponible en: http://www.revistaccuba.cu/index.php/revacc/article/view/3110