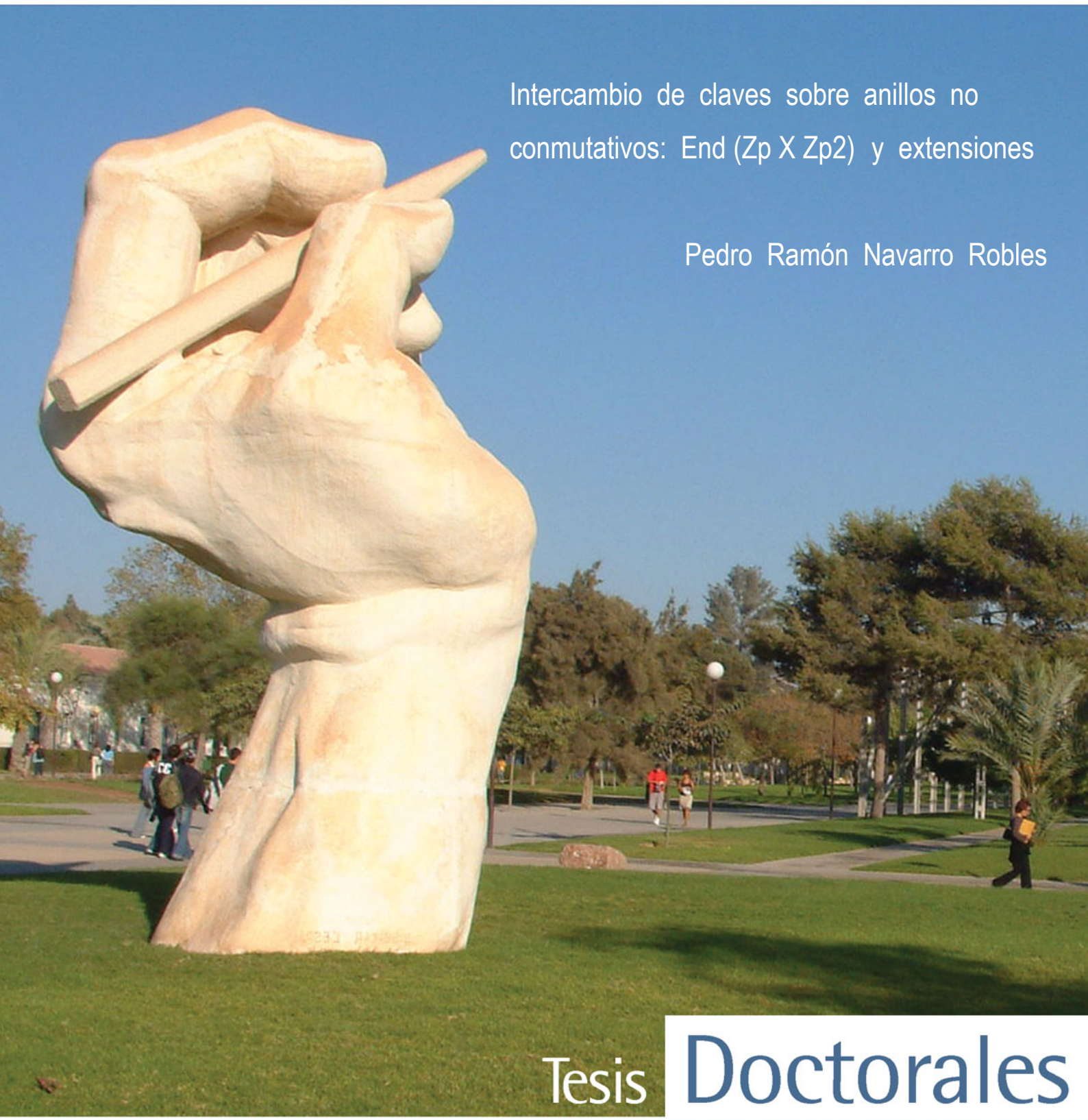
Universitat d'Alacant
Universidad de Alicante

Intercambio de claves sobre anillos no conmutativos: End (Zp X Zp2) y extensiones

Pedro Ramón Navarro Robles



Tesis Doctorales

www.eltallerdigital.com

UNIVERSIDAD de ALICANTE

Universidad de Alicante

Departamento de Ciencia de la Computación e Inteligencia Artificial

Intercambio de claves sobre anillos no conmutativos: $\mathbf{End}(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$ y extensiones

TESIS DOCTORAL

Presentada por:
Pedro Ramón Navarro Robles

Dirigida por:
Joan Josep Climent Coloma
Leandro Tortosa Grau

Universidad de Alicante

Departamento de Ciencia de la Computación e Inteligencia Artificial

Intercambio de claves sobre anillos no conmutativos: $\mathbf{End}(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$ y extensiones

Memoria presentada para optar al grado de doctor por la Universidad de Alicante por Pedro Ramón Navarro Robles.

Alicante, noviembre de 2013.

D. Joan Josep Climent Coloma, Catedrático de Universidad del Departamento de Estadística e Investigación Operativa de la Universidad de Alicante y D. Leandro Tortosa Grau, Profesor Titular del Departamento de Ciencia de la Computación e Inteligencia Artificial de la Escuela Politécnica Superior de la Universidad de Alicante

CERTIFICAN:

Que la presente memoria *Intercambio de claves sobre anillos no conmutativos:* $\mathrm{End}(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$ *y extensiones*, ha sido realizada bajo su dirección, en el Departamento de Ciencia de la Computación e Inteligencia Artificial de la Universidad de Alicante por el licenciado D. Pedro Ramón Navarro Robles, y constituye su tesis para optar al grado de doctor.

Para que conste, en cumplimiento de la legislación vigente, autoriza la presentación de la referida tesis doctoral ante la comisión de Doctorado de la Universidad de Alicante, firmando el presente certificado.

Alicante, 19 de noviembre de 2013

Joan Josep Climent Coloma

Leandro Tortosa Grau

A mis padres,
por todos sus sacrificios para darme una educación pública de calidad.

A Alicia,
por su cariño, apoyo e infinita paciencia en todo momento.

A Ainhoa,
por ser la energía necesaria en todos mis esfuerzos.

Las matemáticas no son una marcha cautelosa a lo largo de una carretera bien despejada, sino un viaje por un desierto desconocido en el que los exploradores se pierden a menudo.

W. S. Anglin. El enigma de Fermat
Editorial Planeta, 2006

En cierto modo esta frase resume muy bien el problema al que se enfrenta cualquier estudiante de doctorado, empezamos adentrándonos en una parte desconocida de las matemáticas siguiendo un sendero que puede haber sido explorado por otros anteriormente, pero del cual no tenemos certeza que tenga el final esperado.

He de expresar mi más sincera gratitud a mis directores de tesis, Joan Josep Climent y Leandro Tortosa por haberme guiado por este sendero donde innumerables veces he estado desorientado y a veces perdido por completo. Dedicándome todo su tiempo, su esfuerzo y su paciencia, haciéndome ver el lado positivo de cada error cometido.

No quiero que mi agradecimiento quede meramente al ámbito académico, quiero agradecerles sus ánimos y su apoyo en aquellos momentos difíciles que he pasado junto a ellos en el ámbito personal, demostrándome su amistad más allá de lo que jamás podría haber imaginado. Gracias de todo corazón.

¿Sabes -confió el diablo- que ni siquiera los mejores matemáticos de otros planetas, todos mucho más avanzados que el tuyo, lo han resuelto? Vamos, hay un tipo en Saturno semejante a una seta con zancos que resuelve mentalmente ecuaciones diferenciales en derivadas parciales; y hasta él ha desistido.

Arthur Poges. El diablo y Simon Flagg.
Richard Simms Publications, 2013

Cuando todo se ve difícil, cuando parece que no hay salida, la ansiedad y la frustración son muy fuertes, pero el apoyo de la gente de nuestro alrededor es la energía necesaria para no desistir e intentarlo una penúltima vez más.

Quiero agradecer a mis padres los sacrificios y el esfuerzo que les supuso darme la posibilidad de tener unos estudios superiores que ellos nunca pudieron permitirse. Espero que os sentáis tan orgullosos de mi como yo de vosotros. Vuestro cariño, comprensión, apoyo y educación en valores, es el mejor regalo que me habéis dado.

Gracias a todos los compañeros de departamento, pero en especial a mi buena amiga, Verónica. Gracias por el apoyo y la disposición que siempre me has mostrado, pero sobretodo por ser la matemática con la que menos he hablado de matemáticas. Se agradece tener a alguien alrededor que de vez en cuando te haga pensar en lo terrenal.

A mi gran amigo Manuel, que nos conocemos desde los años de los dientes de leche y que aún mantenemos una amistad sincera. Gracias por ser mi mejor amigo.

Por último a quien era mi novia cuando empecé esta memoria y ahora se ha convertido en mi mujer cuando la termino, Alicia, que me has dado todo y a quien te debo todo, que me has levantado cuando los días no eran días sino oscuras noches y que siempre has tenido una sonrisa aunque no siempre correspondida como merecías. Cada día te quiero más.

Índice

Capítulo 1

Introducción

1.1 Criptografía de clave pública

Dependiendo del número de claves que utilicen los algoritmos para el cifrado/descifrado de la información, podemos dividir la criptografía en dos grandes areas: la **criptografía de clave privada** o **simétrica** y la **criptografía de clave pública** o **asimétrica**.

En la criptografía de clave privada se dispone de una única clave secreta, que se utiliza para cifrar y descifrar, sobre la que se han puesto de acuerdo las dos partes que quieren comunicarse de forma segura. Una vez compartida la clave, el remitente cifra un mensaje con ella y lo envía al destinatario, que utiliza la misma clave para descifrar el mensaje.

La criptografía de clave pública utiliza dos claves: una privada y otra pública. Cada usuario tiene una clave privada que debe mantener en secreto y otra clave pública que debe difundir entre sus receptores. En una comunicación entre dos usuarios, el emisor cifra los datos con la clave pública del receptor, quien a su vez utiliza su clave privada para descifrar el mensaje recibido.

En esta memoria, nos centramos en el desarrollo e implementación de protocolos criptográficos dentro del ámbito de la criptografía de clave pública, por lo que analizamos con mayor detalle algunos aspectos básicos de la misma.

Actualmente, la mayoría de los criptosistemas de clave pública más conocidos por sus siglas en inglés PKC (*Public Key Cryptosystem*), que se utilizan en nuestro entorno cotidiano se fundamentan en ciertos problemas concretos de la teoría de números. En líneas generales, podemos afirmar que su robustez depende de la difi-

cultad computacional de resolver ciertos problemas matemáticos sobre estructuras algebraicas finitas conmutativas.

De entre estos problemas matemáticos destacamos dos, por la importancia de los criptosistemas que se basan en los mismos.

- El problema de la Factorización Entera o IFP de sus siglas en inglés (*Integer Factorizaton Problem*) que consiste en la dificultad de factorizar un número grande sobre el anillo de los enteros.
- El problema del Logaritmo Discreto o DLP (*Discrete Logarithm Problem*) sobre el cuerpo finito $\mathbb{Z}_p$, con p un primo grande.

El conocido y ampliamente utilizado criptosistema RSA [46] basa su fortaleza en la dificultad de resolver el problema IFP. Debe su nombre a las iniciales de sus autores Rivest, Shamir, Adelman, investigadores del Massachuttes Institue of Technology. Las claves que se utilizan en la mayoría de las implementaciones de RSA son de entre 1024 y 2048 bits de longitud, aunque los expertos recomiendan que n sea como mínimo de 2048 bits, debido a las mejoras constantes en los algoritmos de factorización de números enteros y al aumento de la potencia computacional. Podemos decir, a modo de ejemplo, que RSA es el responsable, junto a otros criptosistemas de clave pública y privada, de la seguridad en Internet, en las transacciones bancarias electrónicas o en la firma digital de correos electrónicos. También es el responsable de la seguridad del DNI-e que funciona en nuestro país.

El conocido protocolo ElGamal [24] y todas sus numerosas variantes basan su fortaleza en el problema DLP. Fue descrito y desarrollado por Taher ElGamal en 1984 y siempre ha sido de uso libre. La seguridad del mismo radica en la dificultad que ofrece el cálculo del logaritmo discreto en grupos cíclicos de tamaño muy grande.

Tanto los esquemas RSA como ElGamal se basan en la resolución de ecuaciones exponenciales en aritmética modular. Sin embargo, en ElGamal, el secreto está incrustado en el exponente, mientras que la base y el resultado son conocidos. En el esquema RSA, el exponente es público y es la base la que constituye el objetivo del atacante, lo que representa la gran diferencia entre ambos protocolos.

Actualmente, la criptografía de clave pública o asimétrica tiene dos aplicaciones fundamentales, como son el intercambio de claves privadas y la firma digital que acompaña a los archivos digitales. En esta memoria nos centramos en las aplicaciones relacionadas con el intercambio de claves.

Desde que Diffie y Hellmann [22] propusieran el primer algoritmo de intercambio de claves, podemos encontrar una bibliografía muy extensa y exhaustiva relacionada con el problema del intercambio de claves. Véase, como ejemplo, [37, 49, 57], así como las referencias incluidas en estos artículos. La mayoría de los protocolos propuestos basan su aritmética sobre estructuras algebraicas conmutativas, sobre las que se ha desarrollado un conjunto de ataques, en gran parte de los casos muy eficientes, basados en la conmutatividad dentro de estas estructuras algebraicas.

Podemos dividir los ataques al problema IFP en dos categorías, según el tipo de algoritmo que utilizan: los de propósito general y los de propósito específico. Los de propósito general son válidos para cualquier entero elegido por el sistema, mientras que los de propósito específico son diseñados para atacar en particular a ciertos enteros.

Entre los ataques de propósito general, destacamos el algoritmo de la criba cuadrática (*Quadratic Sieve*) propuesto por Carl Pormerance [44] en 1982, que es considerado como el más eficiente para números enteros con menos de 100 dígitos. También destacamos el algoritmo de la criba general de los números enteros (*General Number Field Sieve*) diseñado para factorizar enteros con más de 130 dígitos (véase [8]).

Entre los algoritmos de ataque de propósito específico, destaca el algoritmo ρ de Pollard [43] propuesto en 1975, que resulta muy efectivo cuando el entero tiene factores relativamente pequeños. También es destacable el algoritmo de factorización de Lenstra [36], basado en el empleo de curvas elípticas.

En cuanto a los ataques al problema DLP sobre un cuerpo finito $\mathbb{Z}_p$, mencionamos el que probablemente es el más eficaz, el algoritmo *Index-Calculus* basado en las ideas que en 1968 propusieron Western y Miller [60], aunque actualmente atribuido a Kraitchik [33, 34] y Cunningham [20], con todas sus variantes, como la propuesta por Adleman [1] en 1979, dicho algoritmo fundamenta su ataque en la selección de una base irreducible del grupo cíclico y la obtención de un sistema de relaciones lineales con logaritmos discretos en la base, cuya solución nos proporciona el valor buscado. Otros ataques muy eficientes se basan en la idea de encontrar ciclos en secuencias numéricas, cuyo origen es el trabajo de Floyd [25] en 1967, donde propone un algoritmo para encontrar ciclos. Este algoritmo es mejorado por Pollard [42] a mediados de los años 70, de forma que en la actualidad constituye uno de los ataques

más eficientes a los criptosistemas basados en el logaritmo discreto.

Como denominador común podemos afirmar que la base de todos estos ataques se encuentra en la propiedad conmutativa de los elementos del cuerpo finito en el que se define el logaritmo discreto.

Como vemos, el logaritmo discreto y la factorización de enteros están en la base de la mayoría de los protocolos y algoritmos de la criptografía de clave pública, donde incluimos los criptosistemas basados en curvas elípticas. Sin embargo, parece una idea aceptada por los expertos que todos estos algoritmos y protocolos de clave pública basados en estos problemas clásicos de teoría de números pueden resultar inseguros a corto o medio plazo, debido al constante e imparable aumento de la potencia de computación de los ordenadores y estaciones de trabajo actuales. Véase, por ejemplo, [9, 50].

Como consecuencia de estos constantes avances en el terreno de la computación existe, desde hace unos años, un campo activo de investigación que se conoce como criptografía algebraica no conmutativa, en la que se utilizan estructuras matemáticas no conmutativas que nos puedan proporcionar un mayor nivel de seguridad [5, 6]. Para profundizar en diversos aspectos teóricos y prácticos relacionados con la criptografía basada en estructuras no conmutativas, véase [18, 32, 39, 47, 48, 53].

Actualmente, la seguridad de los criptosistemas basados en plataformas criptográficas no conmutativas se basa en alguno de los problemas siguientes:

- **Problema de la búsqueda del conjugador o CSP** (*Conjugator Search Problem*). Dados $(x, y) \in G \times G$, el problema consiste en encontrar $z \in G$ tal que $y = z^{-1}xz$.
- **Problema de la descomposición o DP** (*Descomposition Problem*). Dados $(x, y) \in G \times G$ y $S \subseteq G$, el problema consiste en encontrar $z_1, z_2 \in S$ tales que $y = z_1 x z_2$.
- **Problema de la descomposición simétrica o SDP** (*Symmetrical Decomposition Problem*). Dados $(x, y) \in G \times G$ y $m, n \in \mathbb{Z}$, el problema consiste en encontrar $z \in G$ tal que $y = z^m x z^n$.
- **Problema de la descomposición simétrica generalizado o GSDP** (*Generalized Symmetrical Decomposition Problem*). Dados $(x, y) \in G \times G$, $S \subseteq G$ y $m, n \in \mathbb{Z}$, el problema consiste en encontrar $z \in S$ tal que $y = z^m x z^n$.

Varios autores han propuesto y utilizado ciertos grupos no abelianos para proble-

mas de intercambio de claves. Concretamente, en [5, 4, 32, 31], se sugieren los grupos entrelazados como base de las plataformas criptográficas en las que se implementan los respectivos protocolos. En [41], los autores proponen un esquema PKC cuya seguridad se basa en el problema DLP para el automorfismo definido por la operación de conjugación y la dificultad de encontrar el elemento conjugado en grupos finitos no abelianos.

En [52], se sugiere la utilización de una representación finita de un grupo no abeliano, conocido como grupo de Thomson, con el fin de desarrollar un modelo PKC, fundamentado en la dificultad de resolver el problema SDP. Por otra parte, basado en la dificultad de resolver los problemas CSP y SDP sobre cualquier grupo no conmutativo, podemos ver la propuesta de firma digital de Thomas y Lal [58].

En [28], los autores presentan un criptosistema de clave pública basado en anillos no conmutativos, al que llaman criptosistema NTRU. Este criptosistema es criptoanalizado de forma eficiente en [26, 27]. En [40], los autores introducen el problema del logaritmo discreto para anillos de matrices con elementos en $\mathbb{F}_q$, mientras que un protocolo del tipo Diffie-Hellman de intercambio de claves basado en matrices se puede encontrar en [59]. Menezes y Wu [38] redujeron el problema del logaritmo discreto para matrices a pequeñas extensiones de $\mathbb{F}_q$.

Podemos encontrar un buen número de implementaciones basadas en el protocolo Diffie-Hellman sobre anillos de matrices, para lo cual se utilizan diferentes tipos de matrices [2, 3, 11, 56, 61]. Satoh y Akari [48] presentan un esquema basado en el anillo no conmutativo de los cuaterniones. Cuatro años más tarde, Coppersmith [18] desarrolló algunos ataques sobre este esquema. En [29] se presentan diversos protocolos criptográficos basados en el concepto de anillos de grupo. Se generan unidades en estos anillos que se utilizan como claves públicas, donde las claves secretas son las inversas de estas unidades.

1.2 Esquemas de multidifusión de claves

Actualmente es creciente el interés en las aplicaciones orientadas a las comunicaciones de grupos, lo que ha conducido a los investigadores a la busqueda de protocolos para las comunicaciones de grupo cada vez más eficientes desde el punto de vista computacional pero manteniendo a la vez la seguridad de los mismos en

cuanto a su privacidad e integridad.

Los protocolos de intercambio en un grupo de usuarios o multidifusión, conocidos por modelos *Multicast*, son la forma más eficiente conocida para el envío de información desde un emisor a varios receptores de forma simultánea [21].

Los modelos de multidifusión aplicados sobre redes en dispositivos informáticos, llamados modelos *IP-Multicast*, donde su eficiencia se debe principalmente al hecho de que la información se transmite sólo una vez, para que ésta llegue a todas las direcciones IP receptoras que han mostrado interés en la recepción de la información desde una dirección IP emisora determinada, de forma que pasa por cada conexión entre dos de estos nodos, correspondientes a los receptores [19]. Sin embargo este esquema de distribución de información, aunque es capaz de extenderse cuando el grupo de usuarios crece sin deteriorarse su eficiencia, no ocurre lo mismo cuando tratamos de su seguridad en el acceso a la información distribuida sólo para el grupo de usuarios autorizados. Los esquemas de multidifusión que pretenden mantener seguro el acceso a la información que se intercambia entre los usuarios del grupo son conocidos como sistemas de multidifusión seguros [62] (*Secure Multicast*).

Los modelos de intercambio multidifusión [45] se dividen en tres categorías, dependiendo de las autoridades encargadas de la generación, regeneración, distribución y redistribución de claves en estos modelos:

- **Centralizados**, son los modelos que tienen una autoridad central que se encarga de los cambios de la clave de sesión del esquema.
- **Descentralizados**, aquellos modelos donde existe un grupo de *usuarios independientes* que actúan como autoridades locales para la distribución de claves.
- **Distribuidos**, donde los propios miembros llevan a cabo la distribución y generación de claves de forma coordinada.

1.3 Estructura de la memoria

La principal contribución de esta memoria consiste en el diseño de un conjunto de protocolos de intercambio de claves, así como de esquemas de multidifusión sobre estructuras matemáticas no conmutativas. Para ello, se establece una caracterización del anillo $\mathrm{End}(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$ y una extensión de este anillo, que presenta unas propiedades algebraicas adecuadas para la implementación de protocolos de intercambio claves

con unos niveles de seguridad adecuados.

La memoria se divide en cinco capítulos. En el primero, además de presentar la estrutura de la memoria, se resume de una forma muy concisa los conceptos y características básicas de la criptografía de clave pública de los esquemas de multidifusión de claves, haciendo especial hincapié de los teóricos y prácticos sobre los que se fundamentan los criptosistemas basados en estructuras matemáticas no conmutativas desarrolladas en las últimas décadas.

El segundo capítulo se dedica al estudio de las propiedades algebraicas del anillo de endomorfismos $\mathrm{End}(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$ del grupo aditivo $\mathbb{Z}_p \times \mathbb{Z}_{p^2}$, siendo p un número primo cualquiera, introducido por Bergman [7]. Se introduce un anillo no conmutativo que denotamos por E_p, donde sus elementos se representan mediante matrices de tamaño 2×2 con coeficientes enteros y en el que la aritmética de estos elementos se desarrolla en $\mathbb{Z}_p$ y $\mathbb{Z}_{p^2}$. Se demuestra que E_p es isomorfo al anillo $\mathrm{End}(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$ y se analizan diversas propiedades algebraicas de E_p, así como el cardinal de elementos invertibles. Se observa que el porcentaje de elementos invertibles de E_p crece al aumentar el tamaño del primo p, lo que supone una debilidad en el aspecto de la seguridad, como se pone de manifiesto en el análisis de la seguridad del capítulo 4.

Como consecuencia de esta debilidad desde el punto de vista de la seguridad, en el capítulo 3 se propone una extensión del anillo E_p con el fin de evitar el alto porcentaje de elementos invertibles, especialmente cuando p crece. Se introduce el anillo ${E_p}^{(m)}$ para un cierto número primo p y un cierto número entero $m \geq 2$, donde los elementos son ahora matrices de tamaño $m \times m$, con coeficientes enteros, de forma que E_p coincide con ${E_p}^{(2)}$. En el anillo ${E_p}^{(m)}$ se extiende la aritmética de sus elementos de una forma análoga a como se realiza para E_p. Se obtiene una caracterización de los elementos invertibles de ${E_p}^{(m)}$ y se calcula su número en función de p y de m. Se concluye en este caso que el número de elementos invertibles es prácticamente nulo, para una elección adecuada de p y m.

En el capítulo 4 se desarrollan diversos protocolos de intercambio de claves y esquemas de multidifusión de claves, definidos sobre un anillo cualquiera no conmutativo. En la segunda parte del capítulo se aplican estos protocolos al caso de los anillos E_p y ${E_p}^{(m)}$, realizando un análisis de la seguridad de los mismos. Se presentan dos esquemas de multidifusión de claves, definidos sobre cualquier anillo no conmutativo, en los que se muestra de forma práctica cómo funciona el esquema

en el caso de que un usuario se incorpore al sistema (*operación join*), o en el caso de que un usuario lo abandone (*operación leave*). Se detalla un ejemplo para cada esquema con 4 usuarios sobre el anillo ${E_p}^{(m)}$, para ciertos valores de p y m.

Finalmente, en el último capítulo se resumen las conclusiones de esta memoria y se mencionan las líneas futuras de investigación. La memoria termina con la relación bibliográfica utilizada para su elaboración.

Parte de los resultadas plasmados en esta memoria han sido publicados en distintas revistas [15, 16, 13], algunos continúan en proceso de evaluación para su publicación [17] y otros han sido presentados en distintos congresos y publicados en las correspondientes actas y proceedings [14, 12].

Capítulo 2

El anillo de endormorfismos $\mathrm{End}(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$

2.1 Preliminares

Recordemos que para un entero positivo m, el conjunto $\mathbb{Z}_m = \{0, 1, 2, \ldots, m-1\}$ es un anillo conmutativo y unitario con la adición y la multiplicación módulo m, es decir,

$$x + y = (x + y) \bmod m \quad \text{y} \quad x \cdot y = (xy) \bmod m, \quad \text{para todo} \quad x, y \in \mathbb{Z}_m.$$

Supongamos ahora que p es un número primo y consideremos los anillos $\mathbb{Z}_p$ y $\mathbb{Z}_{p^2}$. Podemos suponer que $\mathbb{Z}_p \subseteq \mathbb{Z}_{p^2}$, aunque $\mathbb{Z}_p$ no es un subanillo de $\mathbb{Z}_{p^2}$. Por tanto, debemos prestar especial atención a la notación, con el fin de prevenir errores de cálculo como el que ponemos de manifiesto seguidamente. Supongamos que $p = 5$, entonces

$$\mathbb{Z}_5 = \{0, 1, 2, 3, 4\} \quad \text{y} \quad \mathbb{Z}_{5^2} = \{0, 1, 2, 3, \ldots, 23, 24\}.$$

Notemos que $2, 4 \in \mathbb{Z}_5$ y $2 + 4 = 1 \in \mathbb{Z}_5$. Pero también $2, 4 \in \mathbb{Z}_{5^2}$ y, en este caso, tenemos que $2 + 4 = 6 \in \mathbb{Z}_{5^2}$. Evidentemente, $1 \neq 6$ en $\mathbb{Z}_{5^2}$. Este error es fácilmente evitable si escribimos, cuando sea necesario, $x \bmod p$ y $x \bmod p^2$ para referirnos al elemento x cuando $x \in \mathbb{Z}_p$ y $x \in \mathbb{Z}_{p^2}$, respectivamente. Así

$$(2 \bmod 5) + (4 \bmod 5) = 1 \bmod 5$$

y

$$(2 \bmod 5^2) + (4 \bmod 5^2) = 6 \bmod 5^2.$$

Otra dificultad con la que nos podemos encontrar es el uso de la notación a^{-1} para expresar el inverso de a. Por ejemplo, $2 \in \mathbb{Z}_5$ y $2 \in \mathbb{Z}_{5^2}$; sin embargo, $2^{-1} = 3$, en $\mathbb{Z}_5$, mientras que $2^{-1} = 13$ en $\mathbb{Z}_{5^2}$.

Por tanto, cuando escribimos 2^{-1} debemos especificar claramente a cual de los dos elementos nos estamos refiriendo, a $3 \in \mathbb{Z}_5$ o a $13 \in \mathbb{Z}_{5^2}$. Podemos salvar esta dificultad si solamente consideramos elementos en $\mathbb{Z}_p$ como veremos seguidamente.

Notemos primero que si $d \in \mathbb{Z}_{p^2}$, entonces, de acuerdo al algoritmo de la división en $\mathbb{Z}$, existe un único par $(u, v) \in \mathbb{Z}_p^2$ tal que $d = pu + v$; por tanto, la aplicación

$$f : \mathbb{Z}_p^2 \longrightarrow \mathbb{Z}_{p^2}, \quad \text{definida como} \quad f(u, v) = pu + v, \quad \text{para todo} \quad (u, v) \in \mathbb{Z}_p^2$$

es biyectiva. Sin embargo, no es un homomorfismo del grupo aditivo $\mathbb{Z}_p^2$ en el grupo aditivo $\mathbb{Z}_{p^2}$, como podemos comprobar con el siguiente ejemplo para $p = 5$, donde tenemos que

$$(2, 3) + (4, 4) = (2 + 4, 3 + 4) = (1, 2) \text{ en } \mathbb{Z}_5^2,$$

con lo que

$$f\left((2, 3) + (4, 4)\right) = f(1, 2) = 5 \cdot 1 + 2 = 7 \text{ en } \mathbb{Z}_{5^2},$$

mientras que

$$f(2, 3) + f(4, 4) = (5 \cdot 2 + 3) + (5 \cdot 4 + 4) = 13 + 24 = 12 \text{ en } \mathbb{Z}_{5^2}.$$

Sin embargo, si reorganizamos los cálculos anteriores como

$$(5 \cdot 2 + 3) + (5 \cdot 4 + 4) = 5 \cdot (2 + 4) + (3 + 4) = 5 \cdot 6 + (5 \cdot 1 + 2) = 5 \cdot (6 + 1) + 2$$

y reducimos módulo 5, el coeficiente de 5, tenemos que

$$(5 \cdot 2 + 3) + (5 \cdot 4 + 4) = 5 \cdot (7 \bmod 5) + 2 = 5 \cdot 2 + 2 = 12 \text{ en } \mathbb{Z}_{5^2},$$

es decir, obtenemos el mismo resultado que en el caso anterior.

Notemos que en este caso, en lugar de reducir módulo 5^2, hemos dividido el término independiente por 5 y hemos añadido una unidad al coeficiente de 5 para finalmente, reducir dicho coeficiente módulo 5.

Este ejemplo sugiere que es posible reorganizar la adición en $\mathbb{Z}_{p^2}$, en términos de la aritmética de $\mathbb{Z}$ y la reducción módulo p. Esto es cierto en general tal como establecemos en el resultado siguiente.

Como es habitual, si $a, b \in \mathbb{Z}$ con $b \neq 0$, denotamos por $\left\lfloor \frac{a}{b} \right\rfloor$ y $a \bmod b$, el cociente y el resto de la división de a entre b, respectivamente.

Lema 2.1: *Supongamos que p es un número primo y consideremos $d_i = pu_i + v_i \in \mathbb{Z}_{p^2}$, con $u_i, v_i \in \mathbb{Z}_p$, para $i = 1, 2$. Si*

$$u = \left(u_1 + u_2 + \left\lfloor \frac{v_1 + v_2}{p} \right\rfloor \right) \bmod p \qquad y \qquad v = (v_1 + v_2) \bmod p,$$

entonces $d_1 + d_2 = pu + v \in \mathbb{Z}_{p^2}$ con $u, v \in \mathbb{Z}_p$.

Demostración: De la definición de u y v tenemos que $u, v \in \mathbb{Z}_p$ y

$$u_1 + u_2 + \left\lfloor \frac{v_1 + v_2}{p} \right\rfloor = p \left\lfloor \frac{u_1 + u_2 + \left\lfloor \frac{v_1 + v_2}{p} \right\rfloor}{p} \right\rfloor + u \quad \text{y} \quad v_1 + v_2 = p \left\lfloor \frac{v_1 + v_2}{p} \right\rfloor + v.$$

Por tanto,

$$\begin{aligned} d_1 + d_2 &= (pu_1 + v_1) + (pu_2 + v_2) \\ &= p(u_1 + u_2) + (v_1 + v_2) \\ &= p(u_1 + u_2) + p \left\lfloor \frac{v_1 + v_2}{p} \right\rfloor + v \\ &= p \left(u_1 + u_2 + \left\lfloor \frac{v_1 + v_2}{p} \right\rfloor \right) + v \\ &= p \left(p \left\lfloor \frac{u_1 + u_2 + \left\lfloor \frac{v_1 + v_2}{p} \right\rfloor}{p} \right\rfloor + u \right) + v \\ &= p^2 \left\lfloor \frac{u_1 + u_2 + \left\lfloor \frac{v_1 + v_2}{p} \right\rfloor}{p} \right\rfloor + pu + v. \end{aligned}$$

Ahora, como $pu + v \in \mathbb{Z}_{p^2}$, por el algoritmo de la división en $\mathbb{Z}$, es evidente que

$$pu + v = (d_1 + d_2) \bmod p^2,$$

es decir, $d_1 + d_2 = pu + v$ en $\mathbb{Z}_{p^2}$. □

Con la multiplicación ocurre algo parecido. Consideremos $13, 24 \in \mathbb{Z}_{5^2}$. Sabemos que

$$(13 \cdot 24) \bmod 5^2 = 12 \in \mathbb{Z}_{5^2}.$$

Ahora bien, como $13 = 5 \cdot 3 + 3$ y $24 = 5 \cdot 4 + 4$, tenemos que

$$\begin{aligned}(5 \cdot 2 + 3) \cdot (5 \cdot 4 + 4) &= 5^2 \cdot 2 \cdot 4 + 5 \cdot (2 \cdot 4 + 4 \cdot 3) + (3 \cdot 4) \\ &= 5^2 \cdot 8 + 5 \cdot (8 + 12) + 5 \cdot 2 + 2 \\ &= 5^2 \cdot 8 + 5 \cdot 22 + 2,\end{aligned}$$

y, mediante las reducciones oportunas, tenemos que

$$(5 \cdot 2 + 3) \cdot (5 \cdot 4 + 4) = 5 \cdot (22 \bmod 5) + 2 = 5 \cdot 2 + 2 = 12 \text{ en } \mathbb{Z}_{5^2}.$$

Mediante un argumento análogo al del lema anterior obtenemos el resultado siguiente.

Lema 2.2: *Supongamos que p es un número primo y consideremos $d_i = pu_i + v_i \in \mathbb{Z}_{p^2}$, con $u_i, v_i \in \mathbb{Z}_p$, para $i = 1, 2$. Si*

$$u = \left(u_1 v_2 + v_1 u_2 + \left\lfloor \frac{v_1 v_2}{p} \right\rfloor \right) \bmod p \quad y \quad v = (v_1 v_2) \bmod p,$$

entonces $d_1 d_2 = pu + v \in \mathbb{Z}_{p^2}$ con $u, v \in \mathbb{Z}_p$.

DEMOSTRACIÓN: De la definición de u y v tenemos que $u, v \in \mathbb{Z}_p$ y

$$u_1 v_2 + u_2 v_1 + \left\lfloor \frac{v_1 v_2}{p} \right\rfloor = p \left\lfloor \frac{u_1 v_2 + u_2 v_1 + \left\lfloor \frac{v_1 v_2}{p} \right\rfloor}{p} \right\rfloor + u \quad \text{y} \quad v_1 v_2 = p \left\lfloor \frac{v_1 v_2}{p} \right\rfloor + v.$$

Por tanto,

$$\begin{aligned}d_1 d_2 &= (pu_1 + v_1) \cdot (pu_2 + v_2) \\ &= p^2 u_1 u_2 + p u_1 v_2 + v_1 p u_2 + v_1 v_2 \\ &= p^2 u_1 u_2 + p(u_1 v_2 + v_1 u_2) + p \left\lfloor \frac{v_1 v_2}{p} \right\rfloor + v\end{aligned}$$

$$= p^2 u_1 u_2 + p\left(u_1 v_2 + v_1 u_2 + \left\lfloor \frac{v_1 v_2}{p} \right\rfloor\right) + v$$

$$= p^2 u_1 u_2 + p\left(p\left\lfloor \frac{u_1 v_2 + v_1 u_2 + \left\lfloor \frac{v_1 v_2}{p} \right\rfloor}{p} \right\rfloor + u\right) + v$$

$$= p^2\left(u_1 u_2 + \left\lfloor \frac{u_1 v_2 + v_1 u_2 + \left\lfloor \frac{v_1 v_2}{p} \right\rfloor}{p} \right\rfloor\right) + pu + v.$$

Ahora, como $pu + v \in \mathbb{Z}_{p^2}$, por el algoritmo de la división en $\mathbb{Z}$, es evidente que

$$pu + v = (d_1 d_2) \bmod p^2,$$

es decir, $d_1 d_2 = pu + v$ en $\mathbb{Z}_{p^2}$. □

Notemos que como consecuencia de los resultados anteriores, es fácil obtener la suma y el producto de los elementos de $\mathbb{Z}_{p^2}$ utilizando solamente la adición y la multiplicación de $\mathbb{Z}$ y $\mathbb{Z}_p$.

El resultado siguiente establece una condición necesaria y suficiente para que un elemento $d = pu + v \in \mathbb{Z}_{p^2}$, con $u, v \in \mathbb{Z}_p$ sea invertible y, además, proporciona una fórmula para calcular $d^{-1} \in \mathbb{Z}_{p^2}$, utilizando solamente la aritmética de $\mathbb{Z}$ y de $\mathbb{Z}_p$.

Lema 2.3: *Supongamos que p es un número primo y consideremos $d = pu+v \in \mathbb{Z}_{p^2}$ con $u, v \in \mathbb{Z}_p$. Entonces, d es invertible en $\mathbb{Z}_{p^2}$ si y sólo si $v \neq 0$ y, en tal caso,*

$$d^{-1} = p\left[\left(-u(v^{-1})^2 - \left\lfloor \frac{vv^{-1}}{p} \right\rfloor v^{-1}\right) \bmod p\right] + v^{-1},$$

donde $v^{-1} \in \mathbb{Z}_p$ es el inverso de v.

Demostración: Supongamos que d es invertible; entonces $\mathrm{mcd}(d, p^2) = 1$. Sin embargo, si $v = 0$ entonces

$$1 = \mathrm{mcd}(d, p^2) = \mathrm{mcd}(pu, p^2) = p,$$

lo cual es una contradicción, por tanto $v \neq 0$.

Recíprocamente, supongamos que $v \neq 0$. Como $\mathbb{Z}_p$ es un cuerpo, existe $v^{-1} \in \mathbb{Z}_p$. Ahora, por el lema 2.2, tenemos que

$$(pu + v)\left\{p\left[\left(-u(v^{-1})^2 - \left\lfloor \frac{vv^{-1}}{p} \right\rfloor v^{-1}\right) \bmod p\right] + v^{-1}\right\}$$

$$= p\left\{uv^{-1} + v\left[\left(-u(v^{-1})^2 - \left\lfloor\frac{vv^{-1}}{p}\right\rfloor v^{-1}\right) \bmod p\right] + \left\lfloor\frac{vv^{-1}}{p}\right\rfloor\right\} \bmod p$$

$$+ (vv^{-1}) \bmod p$$

$$= p\left\{(uv^{-1}) - \left(vu(v^{-1})^2\right) \bmod p - \left(v\left\lfloor\frac{vv^{-1}}{p}\right\rfloor v^{-1}\right) \bmod p\right.$$

$$\left. + \left\lfloor\frac{vv^{-1}}{p}\right\rfloor \bmod p\right\} \bmod p + 1$$

$$= p\left((uv^{-1}) \bmod p - (uv^{-1}) \bmod p - \left\lfloor\frac{vv^{-1}}{p}\right\rfloor \bmod p\right.$$

$$\left. + \left\lfloor\frac{vv^{-1}}{p}\right\rfloor \bmod p\right) \bmod p + 1$$

$$= p \cdot 0 + 1 = 1.$$

Por tanto, $pu + v$ es invertible en $\mathbb{Z}_{p^2}$ y

$$(pu+v)^{-1} = p\left[\left(-u(v^{-1})^2 - \left\lfloor\frac{vv^{-1}}{p}\right\rfloor\right) \bmod p\right] + v^{-1}. \qquad \square$$

Notemos que la expresión anterior puede resultar confusa ya que nos puede llevar a suponer que

$$\left\lfloor\frac{vv^{-1}}{p}\right\rfloor \bmod p = \left\lfloor\frac{(vv^{-1}) \bmod p}{p}\right\rfloor = \left\lfloor\frac{1}{p}\right\rfloor = 0,$$

que es falso, como podemos ver si tomamos $p = 5$ y $v = 2$; entonces $v^{-1} = 3$ y

$$\left\lfloor\frac{vv^{-1}}{p}\right\rfloor \bmod p = \left\lfloor\frac{2 \cdot 3}{5}\right\rfloor \bmod 5 = \left\lfloor\frac{6}{5}\right\rfloor = 1.$$

2.2 Caracterización del anillo $\mathrm{End}(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$

Para un número primo p consideramos el grupo aditivo $\mathbb{Z}_p \times \mathbb{Z}_{p^2}$, de orden p^3, donde la adición se define componente a componente. Consideremos también el conjunto $\mathrm{End}(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$ de los endomorfismos de dicho grupo aditivo. Es bien conocido que $\mathrm{End}(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$ un anillo unitario y no conmutativo con la adición y la composición usuales de endomorfismos definidos, para $f, g \in \mathrm{End}(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$ como

$$(f+g)(x,y) = f(x,y) + g(x,y) \quad \text{y} \quad (f \circ g)(x,y) = f(g(x,y)).$$

Las identidades aditiva y multiplicativa, que denotamos por O y I respectivamente se definen, obviamente, como

$$O(x, y) = (0, 0) \quad \text{e} \quad I(x, y) = (x, y).$$

Bergman [7] estableció que el anillo de endomorfismos $\mathrm{End}(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$ es un anillo semilocal con p^5 elementos que no se puede embeber en un anillo de matrices sobre un anillo conmutativo. Enunciamos dicho resultado para futuras referencias.

Teorema 2.1 (Teorema 3 de [7]): *Si p es un número primo, entonces el anillo de endomorfismos $\mathrm{End}(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$ tiene p^5 elementos, es semilocal y no puede ser embebido en ningún anillo de matrices sobre un anillo conmutativo.*

Recordemos que un anillo es semilocal si el cociente por su radical de Jacobson es artiniano y semisimple (véase, por ejemplo, [35], para un estudio más detallado de las propiedades de los anillos no conmutativos).

Ahora introducimos unos endomorfismos de $\mathbb{Z}_p \times \mathbb{Z}_{p^2}$ que nos permitirán caracterizar los elementos de $\mathrm{End}(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$ como combinaciones lineales de dichos endomorfismos con coeficientes en $\mathbb{Z}_p$ y $\mathbb{Z}_{p^2}$.

Consideremos las proyecciones

$$\pi_1 : \mathbb{Z}_p \times \mathbb{Z}_{p^2} \longrightarrow \mathbb{Z}_p \quad \text{y} \quad \pi_2 : \mathbb{Z}_p \times \mathbb{Z}_{p^2} \longrightarrow \mathbb{Z}_{p^2}$$

que podemos extender, de forma natural, a sendos endormorfismos de $\mathbb{Z}_p \times \mathbb{Z}_{p^2}$, que volvemos a denotar por π_1 y π_2 respectivamente, como

$$\pi_1(x, y) = (x, 0) \quad \text{y} \quad \pi_2(x, y) = (0, y).$$

Consideremos también la aplicación cociente $\sigma : \mathbb{Z}_{p^2} \longrightarrow \mathbb{Z}_p$ y la inmersión natural $\tau : \mathbb{Z}_p \longrightarrow \mathbb{Z}_{p^2}$ que podemos definir respectivamente como $\sigma(y) = y \bmod p$ y $\tau(x) = px$.

Podemos extender dichas aplicaciones, de forma natural, a sendos endormorfismos de $\mathbb{Z}_p \times \mathbb{Z}_{p^2}$, que denotamos por σ y τ respectivamente, como

$$\sigma(x, y) = (y \bmod p, 0) \quad \text{y} \quad \tau(x, y) = (0, px).$$

Ahora estamos en condiciones de establecer el resultado siguiente.

Teorema 2.2: *Los endomorfismos π_1, π_2, τ y σ verifican las siguientes identidades:*

$$\begin{array}{llll} \pi_1 \circ \pi_1 = \pi_1, & \pi_1 \circ \pi_2 = O, & \pi_1 \circ \tau = O, & \pi_1 \circ \sigma = \sigma, \\ \pi_2 \circ \pi_1 = O, & \pi_2 \circ \pi_2 = \pi_2, & \pi_2 \circ \tau = \tau, & \pi_2 \circ \sigma = O, \\ \tau \circ \pi_1 = \tau, & \tau \circ \pi_2 = O, & \tau \circ \tau = O, & \tau \circ \sigma = p\pi_2, \\ \sigma \circ \pi_1 = O, & \sigma \circ \pi_2 = \sigma, & \sigma \circ \tau = O, & \sigma \circ \sigma = O, \end{array}$$

donde $p\pi_2$ es la suma de π_2 consigo mismo p veces. Además, el orden aditivo de π_1, σ y τ es p, mientras que el orden aditivo de π_2 es p^2.

DEMOSTRACIÓN: Supongamos que $(x, y) \in \mathbb{Z}_p \times \mathbb{Z}_{p^2}$. De acuerdo con las definiciones de π_1, π_2, σ y τ tenemos que

$$(\pi_1 \circ \pi_1)(x, y) = \pi_1(\pi_1(x, y)) = \pi_1(x, 0) = (x, 0) = \pi_1(x, y),$$

$$(\pi_2 \circ \tau)(x, y) = \pi_2(\tau(x, y)) = \pi_2(0, px) = (0, px) = \tau(x, y),$$

$$\begin{aligned} (\tau \circ \sigma)(x, y) &= \tau(\sigma(x, y)) = \tau(y \bmod p, 0) = (0, p(y \bmod p)) = (0, py) \\ &= p(0, y) = p\pi_2(x, y) = (p\pi_2)(x, y), \end{aligned}$$

$$(\sigma \circ \pi_2)(x, y) = \sigma(\pi_2(x, y)) = \sigma(0, y) = (y \bmod p, 0) = \sigma(x, y).$$

Por tanto, $\pi_1 \circ \pi_1 = \pi_1$, $\pi_2 \circ \tau = \tau$, $\tau \circ \sigma = p\pi_2$ y $\sigma \circ \pi_2 = \sigma$.

Mediante un razonamiento análogo podemos probar el resto de identidades. Supongamos ahora que k es un entero positivo. Puesto que

$$(k\pi_1)(x, y) = (kx, 0), \quad (k\sigma)(x, y) = (ky, 0) \quad \text{y} \quad (k\tau)(x, y) = (0, kpx),$$

tenemos que $k\pi_1 = O$, $k\sigma = O$ y $k\tau = O$ si y sólo si $p \mid k$. Por tanto, el orden aditivo de π_1, σ y τ es p.

Por último, como $(k\pi_2)(x, y) = (0, ky)$, tenemos que $k\pi_2 = O$ si y sólo si $p^2 \mid k$ y, por tanto, el orden aditivo de π_2 es p^2. □

Como consecuencia de los teoremas 2.1 y 2.2, podemos establecer la siguiente caracterización de los elementos de $\mathrm{End}(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$.

Teorema 2.3: *Si p es un número primo, entonces*

$$\mathrm{End}(\mathbb{Z}_p \times \mathbb{Z}_{p^2}) = \{a\pi_1 + b\sigma + c\tau + d\pi_2 \mid a, b, c \in \mathbb{Z}_p \text{ y } d \in \mathbb{Z}_{p^2}\},$$

donde π_1, σ, τ y π_2 son los endomorfismos introducidos anteriormente.

Demostración: Supongamos que $a, b, c \in \mathbb{Z}_p$ y $d \in \mathbb{Z}_{p^2}$. Puesto que $\pi_1, \sigma, \tau, \pi_2 \in \mathrm{End}(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$, es evidente que

$$a\pi_1 + b\sigma + c\tau + d\pi_2 \in \mathrm{End}(\mathbb{Z}_p \times \mathbb{Z}_{p^2}).$$

Por tanto,

$$\{a\pi_1 + b\sigma + c\tau + d\pi_2 \mid a, b, c \in \mathbb{Z}_p \text{ y } d \in \mathbb{Z}_{p^2}\} \subseteq \mathrm{End}(\mathbb{Z}_p \times \mathbb{Z}_{p^2}).$$

Si para algunos $a, b, c, a', b', c' \in \mathbb{Z}_p$ y $d, d' \in \mathbb{Z}_{p^2}$ tenemos que

$$a\pi_1 + b\sigma + c\tau + d\pi_2 = a'\pi_1 + b'\sigma + c'\tau + d'\pi_2$$

entonces

$$(a\pi_1 + b\sigma + c\tau + d\pi_2)(1, 0) = (a'\pi_1 + b'\sigma + c'\tau + d'\pi_2)(1, 0),$$

es decir, $(a, pc) = (a', pc')$ y, en consecuencia, $a = a'$ y $c = c'$.

Análogamente,

$$(a\pi_1 + b\sigma + c\tau + d\pi_2)(0, 1) = (a'\pi_1 + b'\sigma + c'\tau + d'\pi_2)(0, 1),$$

es decir, $(b, d) = (b', d')$, por tanto $b = b'$ y $d = d'$.

Esto nos permite afirmar que

$$\mathrm{Card}\,(a\pi_1 + b\sigma + c\tau + d\pi_2 \mid a, b, c \in \mathbb{Z}_p \text{ y } d \in \mathbb{Z}_{p^2}) = p^5.$$

Ahora, como por el teorema [7], $\mathrm{Card}\,(\mathrm{End}(\mathbb{Z}_p \times \mathbb{Z}_{p^2})) = p^5$, necesariamente,

$$\mathrm{End}(\mathbb{Z}_p \times \mathbb{Z}_{p^2}) = \{a\pi_1 + b\sigma + c\tau + d\pi_2 \mid a, b, c \in \mathbb{Z}_p \text{ y } d \in \mathbb{Z}_{p^2}\}. \qquad \square$$

2.3 El anillo E_p

2.3.1 Caracterización de E_p

El teorema 2.1 establece que el anillo $\mathrm{End}(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$ no se puede embeber en ningún anillo de matrices sobre un anillo conmutativo. Sin embargo, como veremos seguidamente, podemos obtener una representación matricial de los elementos de dicho anillo.

Teorema 2.4: *Supongamos que p es un número primo. El conjunto*

$$E_p = \left\{ \begin{bmatrix} a & b \\ pc & d \end{bmatrix} \mid a, b, c \in \mathbb{Z}_p \quad y \quad d \in \mathbb{Z}_{p^2} \right\}$$

es un anillo unitario no conmutativo con la adición y el producto definidos como

$$\begin{bmatrix} a_1 & b_1 \\ pc_1 & d_1 \end{bmatrix} + \begin{bmatrix} a_2 & b_2 \\ pc_2 & d_2 \end{bmatrix} = \begin{bmatrix} (a_1 + a_2) \bmod p & (b_1 + b_2) \bmod p \\ [p(c_1 + c_2)] \bmod p^2 & (d_1 + d_2) \bmod p^2 \end{bmatrix} \tag{2.1}$$

y

$$\begin{bmatrix} a_1 & b_1 \\ pc_1 & d_1 \end{bmatrix} \cdot \begin{bmatrix} a_2 & b_2 \\ pc_2 & d_2 \end{bmatrix} = \begin{bmatrix} (a_1 a_2) \bmod p & (a_1 b_2 + b_1 d_2) \bmod p \\ [p(c_1 a_2 + d_1 c_2)] \bmod p^2 & (pc_1 b_2 + d_1 d_2) \bmod p^2 \end{bmatrix} \tag{2.2}$$

respectivamente.

Demostración: La demostración es una simple comprobación. □

Puesto que $\mathbb{Z}_p \subseteq \mathbb{Z}_{p^2}$, podemos considerar que $E_p \subseteq \mathrm{Mat}_2(\mathbb{Z}_{p^2})$. Sin embargo, E_p de acuerdo con el teorema anterior, E_p no puede ser un subanillo de $\mathrm{Mat}_2(\mathbb{Z}_{p^2})$.

Notemos también que la adición y la multiplicación de elementos de E_p son análogas a la adición y multiplicación de matrices de tamaño 2×2 con elementos en $\mathbb{Z}$, con la particularidad de que los elementos de la primera fila se reducen módulo p, mientras que los elementos de la segunda fila se reducen módulo p^2.

Del teorema anterior tenemos que

$$O = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \qquad \text{e} \qquad I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix},$$

son las identidades aditiva y multiplicativa de E_p, respectivamente.

Además, si tenemos en cuenta cómo se calculan los opuestos en $\mathbb{Z}_p$ y $\mathbb{Z}_{p^2}$, es evidente que el opuesto de

$$\begin{bmatrix} a & b \\ pc & d \end{bmatrix} \in E_p \quad \text{es} \quad \begin{bmatrix} p-a & p-b \\ p(p-c) & p^2-d \end{bmatrix} \in E_p. \tag{2.3}$$

En la sección siguiente estableceremos una caracterización de los elementos invertibles de E_p.

Por otro lado, notemos que como consecuencia del teorema 2.3, si tomamos $f \in \mathrm{End}(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$, entonces, existe una única 4-tupla $(a, b, c, d) \in \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_{p^2}$ tal que

$$f = a\pi_1 + b\sigma + c\tau + d\pi_2.$$

Ahora, si utilizamos esta caracterización de los elementos de $\mathrm{End}(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$, podemos asegurar que el anillo introducido en el teorema 2.4, es isomorfo al anillo $\mathrm{End}(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$.

Teorema 2.5: *Supongamos que p es un número primo. La aplicación*

$\Phi : \mathrm{End}(\mathbb{Z}_p \times \mathbb{Z}_{p^2}) \longrightarrow E_p$ *definida como*

$$\Phi\left(a\pi_1 + b\sigma + c\tau + d\pi_2\right) = \begin{bmatrix} a & b \\ pc & d \end{bmatrix} \tag{2.4}$$

es un isomorfismo de anillos.

Demostración: Por el teorema 2.3, Φ es una aplicación biyectiva.

Supongamos que $f, g \in \mathrm{End}(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$. Como consecuencia de los teoremas 2.2 y 2.3, si

$$f = a_1\pi_1 + b_1\sigma + c_1\tau + d_1\pi_2 \quad \text{y} \quad g = a_2\pi_1 + b_2\sigma + c_2\tau + d_2\pi_2,$$

entonces

$$\begin{aligned} f+g =&(a_1\pi_1+b_1\sigma+c_1\tau+d_1\pi_2)+(a_2\pi_1+b_2\sigma+c_2\tau+d_2\pi_2)\\ =&\left((a_1+a_2) \bmod p\right)\pi_1+\left((b_1+b_2) \bmod p\right)\sigma\\ &+\left((c_1+c_2) \bmod p\right)\tau+\left((d_1+d_2) \bmod p^2\right)\pi_2 \end{aligned} \tag{2.5}$$

y

$$\begin{aligned} f\circ g =&(a_1\pi_1+b_1\sigma+c_1\tau+d_1\pi_2)\circ(a_2\pi_1+b_2\sigma+c_2\tau+d_2\pi_2)\\ =&a_1a_2(\pi_1\circ\pi_1)+a_1b_2(\pi_1\circ\sigma)+a_1c_2(\pi_1\circ\tau)+a_1d_2(\pi_1\circ\pi_2)\\ &+b_1a_2(\sigma\circ\pi_1)+b_1b_2(\sigma\circ\sigma)+b_1c_2(\sigma\circ\tau)+b_1d_2(\sigma\circ\pi_2)\\ &+c_1a_2(\tau\circ\pi_1)+c_1b_2(\tau\circ\sigma)+c_1c_2(\tau\circ\tau)+c_1d_2(\tau\circ\pi_2)\\ &+d_1a_2(\pi_2\circ\pi_1)+d_1b_2(\pi_2\circ\sigma)+d_1c_2(\pi_2\circ\tau)+d_1d_2(\pi_2\circ\pi_2)\\ =&\left((a_1a_2) \bmod p\right)\pi_1+\left((a_1b_2+b_1d_2) \bmod p\right)\sigma\\ &+\left((c_1a_2+d_1c_2) \bmod p\right)\tau+\left((pc_1b_2+d_1d_2) \bmod p^2\right)\pi_2. \end{aligned} \tag{2.6}$$

Ahora, de las expresiones (2.4), (2.5) y (2.1) tenemos que

$$\Phi(f+g)=\Phi(f)+\Phi(g).$$

Análogamente, de las expresiones (2.4), (2.6) y (2.2) tenemos que

$$\Phi(f\circ g)=\Phi(f)\cdot\Phi(g).$$

En consecencia, Φ es un homomorfismo de anillos. □

A partir de este momento podemos identificar los elementos de $\mathrm{End}(\mathbb{Z}_p\times\mathbb{Z}_{p^2})$ con los elementos de E_p y la aritmética de $\mathrm{End}(\mathbb{Z}_p\times\mathbb{Z}_{p^2})$ con la aritmética de E_p. En particular, $\mathrm{Card}\,(E_p)=p^5$.

Dado que en el anillo E_p trabajamos con elementos de $\mathbb{Z}_p$ y de $\mathbb{Z}_{p^2}$, el hecho de que $\mathbb{Z}_p\subseteq\mathbb{Z}_{p^2}$, representa, como hemos mencionado en la sección 2.1, una dificultad con la notación de algunos elementos. Ahora bien, como consecuencia de los lemas

2.2 y 2.3, podemos salvar dicha dificultad ya que dicos resultados nos permiten trabajar solamente con elementos de $\mathbb{Z}_p$. Antes de continuar, notemos que

$$E_p = \left\{ \begin{bmatrix} a & b \\ pc & pu+v \end{bmatrix} \mid a,b,c,u,v \in \mathbb{Z}_p \right\}.$$

El resultado siguiente es una consecuencia inmediata de los lemas 2.2 y 2.3 y de la expresión anterior.

Teorema 2.6: *Supongamos que p es un número primo. Si*

$$\begin{bmatrix} a_1 & b_1 \\ pc_1 & pu_1+v_1 \end{bmatrix}, \quad \begin{bmatrix} a_2 & b_2 \\ pc_2 & pu_2+v_2 \end{bmatrix} \in E_p, \text{ entonces}$$

$$\begin{bmatrix} a_1 & b_1 \\ pc_1 & pu_1+v_1 \end{bmatrix} + \begin{bmatrix} a_2 & b_2 \\ pc_2 & pu_2+v_2 \end{bmatrix}$$

$$= \begin{bmatrix} (a_1+a_2) \bmod p & (b_1+b_2) \bmod p \\ p\left[(c_1+c_2) \bmod p\right] & p\left[\left(u_1+u_2+\left\lfloor \frac{v_1+v_2}{p} \right\rfloor\right) \bmod p\right] + (v_1+v_2) \bmod p \end{bmatrix},$$

$$\begin{bmatrix} a_1 & b_1 \\ pc_1 & pu_1+v_1 \end{bmatrix} \cdot \begin{bmatrix} a_2 & b_2 \\ pc_2 & pu_2+v_2 \end{bmatrix}$$

$$= \begin{bmatrix} (a_1a_2) \bmod p & (a_1b_2+b_1v_2) \bmod p \\ p\left[(c_1a_2+v_1c_2) \bmod p\right] & p\left[\left(c_1b_2+u_1v_2+v_1u_2+\left\lfloor \frac{v_1v_2}{p} \right\rfloor\right) \bmod p\right] + (v_1v_2) \bmod p \end{bmatrix}.$$

Demostración: La demostración es consecuencia inmediata de las expresiones (2.1) y (2.2) para la adición y la multiplicación, respectivamente, y el uso de los lemas 2.1 y 2.2 para la adición y multiplicación de elementos de $\mathbb{Z}_{p^2}$. □

2.3.2 Elementos invertibles en E_p

Como hemos comentado anteriormente, en esta sección caracterizamos los elementos invertibles de E_p y calculamos su número.

Teorema 2.7: *Supongamos que p es un número primo y $M = \begin{bmatrix} a & b \\ pc & pu+v \end{bmatrix} \in E_p$ con $a, b, c, u, v \in \mathbb{Z}_p$. M es invertible si y sólo si $a \neq 0$ y $v \neq 0$ y, en tal caso, $M^{-1} = \begin{bmatrix} x_{11} & x_{12} \\ x_{21} & x_{21} \end{bmatrix}$ con*

$$x_{11} = a^{-1} \tag{2.7}$$

$$x_{12} = (-a^{-1}bv^{-1}) \bmod p \tag{2.8}$$

$$x_{21} = p\left[(-v^{-1}ca^{-1}) \bmod p\right] \tag{2.9}$$

$$x_{22} = p\left[\left(ca^{-1}b(v^{-1})^2 - u(v^{-1})^2 - \left\lfloor \frac{vv^{-1}}{p} \right\rfloor v^{-1}\right) \bmod p\right] + v^{-1} \tag{2.10}$$

DEMOSTRACIÓN: Supongamos que M es invertible. Entonces existe un elemento $\begin{bmatrix} x & y \\ pz & pr+s \end{bmatrix} \in E_p$, con $x, y, z, r, s \in \mathbb{Z}_p$, tal que

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} a & b \\ pc & pu+v \end{bmatrix} \begin{bmatrix} x & y \\ pz & pr+s \end{bmatrix}.$$

Ahora, por el teorema 2.6,

$$1 = (ax) \bmod p \quad \text{y} \quad 1 = (vs) \bmod p,$$

con lo que $a \neq 0$ y $v \neq 0$.

Recíprocamente, supongamos ahora que $a \neq 0$ y $v \neq 0$, entonces, existen $a^{-1}, v^{-1} \in \mathbb{Z}_p$. Supongamos que $N \in E_p$ es el elemento definido por las expresiones de (2.7) a (2.10). Entonces por el teorema 2.6, tenemos que $MN = \begin{bmatrix} x & y \\ pz & t \end{bmatrix}$, donde

$$x = (aa^{-1}) \bmod p = 1,$$

$$y = \left[a(-a^{-1}bv^{-1}) + bv^{-1}\right] \bmod p = \left(-bv^{-1} + bv^{-1}\right) \bmod p = 0,$$

$$z = \left[ca^{-1} + v(-v^{-1}ca^{-1})\right] \bmod p = \left(ca^{-1} - ca^{-1}\right) \bmod p = 0,$$

$$\begin{aligned} t &= p\left\{\left[c(-a^{-1}bv^{-1}) + uv^{-1} + v\left(ca^{-1}b(v^{-1})^2 - u(v^{-1})^2 - \left\lfloor \frac{vv^{-1}}{p} \right\rfloor v^{-1}\right) + \right.\right. \\ &\quad \left.\left. \left\lfloor \frac{vv^{-1}}{p} \right\rfloor\right] \bmod p\right\} + (vv^{-1}) \bmod p \\ &= p\left[\left(-ca^{-1}bv^{-1} + uv^{-1} + ca^{-1}bv^{-1} - uv^{-1} - \left\lfloor \frac{vv^{-1}}{p} \right\rfloor + \left\lfloor \frac{vv^{-1}}{p} \right\rfloor\right) \bmod p\right] + 1 \\ &= p \cdot 0 + 1 = 1. \end{aligned}$$

Por tanto, $MN = I$.

Mediante un argumento completamente análogo tenemos que $NM = I$ y, en consecuencia, M es invertible y $M^{-1} = N$. □

Una vez caracterizados los elementos invertibles de E_p, nos preguntamos cuántos elementos de E_p son invertibles para cada valor de p. El resultado siguiente proporciona la respuesta a dicha pregunta.

Teorema 2.8: *El número de elementos invertibles de E_p es $p^3(p-1)^2$.*

DEMOSTRACIÓN: Para determinar el número de elementos invertibles $\begin{bmatrix} a & b \\ pc & pu+v \end{bmatrix}$ de E_p contamos los elementos no invertibles, es decir, de acuerdo con el teorema 2.2, aquellos elementos para los que $a = 0$ o $v = 0$.

Claramente, el número de elementos de la forma $\begin{bmatrix} 0 & b \\ pc & pu+v \end{bmatrix}$ es p^4. También, el número de elementos de la forma $\begin{bmatrix} a & b \\ pc & pu \end{bmatrix}$ es p^4. Ahora, restamos los p^3 elementos de la forma $\begin{bmatrix} 0 & b \\ pc & pu \end{bmatrix}$, tenemos que el número total de elementos no invertibles en

E_p es $2p^4 - p^3$. Por tanto, concluimos que el número de elementos invertibles en E_p es

$$p^5 - 2p^4 + p^3 = p^3(p-1)^2. \qquad \square$$

Puesto que

$$\frac{p^3(p-1)^2}{p^5} = \left(\frac{p-1}{p}\right)^2 \approx 1,$$

podemos afirmar que para valores grandes de p, práticamente todos los elementos de E_p son invertibles.

La tabla 2.1 muestra el porcentaje de elementos invertibles de E_p para algunos valores de p. Notemos que para $p = 211$ el número de elementos invertibles representa el 99 % de los elementos de E_{211}. Sin embargo, para valores de p con 5 dígitos (por ejemplo, $p = 20011$) el número de elementos invertibles representa el 99, 99 %.

Notemos que incluso para valores pequeños de p, el número de elementos invertibles de E_p es muy alto. Por tanto, si tomamos el valor de p con 3 dígitos, la probabilidad de que un elemento de E_p sea invertible es superior al 98 %.

2.3.3 Otras propiedades

En esta sección recogemos algunas propiedades de E_p que utilizaremos en el capítulo 4.

Teorema 2.9: *Si p es un número primo, entonces el centro de E_p es el conjunto*

$$Z(E_p) = \left\{ \begin{bmatrix} x & 0 \\ 0 & py+x \end{bmatrix} \in E_p, \ \mid \ x, y \in \mathbb{Z}_p \right\}. \tag{2.11}$$

y, por tanto, $\text{Card}\,(Z(E_p)) = p^2$.

Demostración: Supongamos que $\begin{bmatrix} a & b \\ pc & pu+v \end{bmatrix}, \quad \begin{bmatrix} x & 0 \\ 0 & py+x \end{bmatrix} \in E_p,$

con $a, b, c, u, v, x, y \in \mathbb{Z}_p$. Puesto que $(py+x)pc \bmod p^2 = pcx \bmod p^2$, tenemos que

$$\begin{bmatrix} a & b \\ pc & pu+v \end{bmatrix} \cdot \begin{bmatrix} x & 0 \\ 0 & py+x \end{bmatrix} = \begin{bmatrix} ax & bx \\ pcx & (pu+v)(py+x) \end{bmatrix}$$

$$= \begin{bmatrix} xa & xb \\ (py+x)pc & (py+x)(pu+v) \end{bmatrix} = \begin{bmatrix} x & 0 \\ 0 & py+x \end{bmatrix} \cdot \begin{bmatrix} a & b \\ pc & pu+v \end{bmatrix}$$

con lo que $\begin{bmatrix} x & 0 \\ 0 & py+x \end{bmatrix} \in Z(E_p)$.

Ahora es fácil comprobar que cualquier elemento que no tenga dicha forma, no puede pertenecer al $Z(E_p)$.

En consecuencia, se satisface la expresión 2.11.

Finalmente, de la expresión 2.11 tenemos que $\mathrm{Card}(Z(E_p)) = p^2$. □

Además, si $u_1, u_2 \in \mathbb{Z}_p \setminus \{0\}$, entonces

$$\begin{bmatrix} 0 & 0 \\ 0 & pu_1 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 0 & pu_2 \end{bmatrix} \in Z(E_p) \setminus \{0\}$$

y como

$$\begin{bmatrix} 0 & 0 \\ 0 & pu_1 \end{bmatrix} \begin{bmatrix} 0 & 0 \\ 0 & pu_2 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & p^2u_1u_2 \mod p^2 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

tenemos que $Z(E_p)$, y por tanto, también E_p tienen divisores de cero. En consecuencia, ni $Z(E_p)$ ni E_p son dominios de integridad ni pueden ser, por tanto, anillos euclidianos ninguno de ellos.

p	Elementos en E_p	Número de elementos invertibles	%
2	32	8	25, 0000
3	243	108	44, 4444
5	3 125	2 000	64, 0000
7	16 807	12 348	73, 4694
11	161 051	133 100	82, 6446
13	371 293	316 368	85, 2071
17	1 419 857	1 257 728	88, 5813
19	2 476 099	2 222 316	89, 7507
23	6 436 343	5 888 828	91, 4934
⋮	⋮	⋮	⋮
97	8 587 340 257	8 411 194 368	97, 9488
101	10 510 100 501	10 303 010 000	98, 0296
103	11 592 740 743	11 368 731 708	98, 0677
107	14 025 517 307	13 764 583 148	98, 1396
109	15 386 239 549	15 105 218 256	98, 1736
113	18 424 351 793	18 099 699 968	98, 2379
127	33 038 369 407	32 520 128 508	98, 4314
131	38 579 489 651	37 992 737 900	98, 4791
137	48 261 724 457	47 559 745 088	98, 5455
⋮	⋮	⋮	⋮
211	418 227 202 051	414 272 357 100	99, 0544
223	551 473 077 343	546 538 220 028	99, 1051
227	602 738 989 907	597 440 211 308	99, 1209
229	629 763 392 149	624 275 284 176	99, 1286
233	686 719 856 393	680 837 914 688	99, 1435
⋮	⋮	⋮	⋮
1009	1 045 817 322 864 049	1 043 745 372 262 656	99, 8019
1013	1 066 712 113 176 293	1 064 607 107 052 368	99, 8027
1019	1 098 679 244 081 099	1 096 523 915 038 316	99, 8038
1021	1 109 503 586 489 101	1 107 331 284 344 400	99, 8042
1031	1 164 912 556 234 151	1 162 653 879 971 900	99, 8061
⋮	⋮	⋮	⋮
10007	100 350 490 343 120 066 807	100 330 435 286 394 092 348	99, 9800
10501	127 688 943 139 852 552 501	127 664 624 910 485 250 000	99, 9810
20011	3 208 809 685 325 464 261 051	3 208 488 388 757 658 533 100	99, 9900
40009	102 524 251 851 665 312 259 049	102 516 127 306 153 088 686 656	99, 9950
60013	778 442 765 119 100 568 670 293	778 416 822 863 939 144 476 368	99, 9967
⋮	⋮	⋮	⋮

Tabla 2.1: *Porcentaje de elementos invertibles de E_p para algunos valores de p*

Capítulo 3

Una extensión del anillo E_p

3.1 Preliminares

A pesar de las buenas propiedades del anillo E_p estudiado en el capítulo 2, como veremos en el capítulo 4, también tiene otras propiedades que no lo hacen apto para algunas aplicaciones criptográficas. Por ello, en este capítulo introducimos un nuevo anillo que mantiene las buenas propiedades de E_p y elimina las propiedades que lo hacen inadecuado para las aplicaciones criptográficas que se proponen.

Supongamos que p es un número primo y que $m \geq 2$ es un entero. En esta sección consideramos la siguiente cadena de inclusiones entre conjuntos

$$\mathbb{Z}_p \subseteq \mathbb{Z}_{p^2} \subseteq \mathbb{Z}_{p^3} \subseteq \cdots \subseteq \mathbb{Z}_{p^{m-1}} \subseteq \mathbb{Z}_{p^m} \subseteq \mathbb{Z}. \tag{3.1}$$

Notemos que la cadena de inclusiones anterior no implica que consideremos cada uno de los anillos anteriores como un subanillo del anillo siguiente en la cadena.

De la misma forma que en el capítulo 2 con el anillo E_p, en esta sección introducimos una serie de resultados que serán útiles para el desarrollo del resto del capítulo.

Para cualquier entero positivo t, como consecuencia del algoritmo de la división en $\mathbb{Z}$, podemos expresar cualquier elemento $a \in \mathbb{Z}_{p^t}$ de forma única como

$$a = \sum_{k=0}^{t-1} p^k a_k, \text{ con } a \in \mathbb{Z}_p, \text{ para } k = 0, 1, \ldots, t-1.$$

A continuación introducimos una serie de resultados a través de una observación un par de lemas, que generalizan los lemas 2.1 y 2.2 demostrados en el capítulo 2, a

partir de los cuales podemos definir la aritmética en $\mathbb{Z}_{p^t}$ en función únicamente de la aritmética de $\mathbb{Z}$ y la reducción módulo p.

Observación 3.1: Supongamos que $a, b \in \mathbb{Z}_{p^t}$, para un entero positivo t. Entonces

$$a = \sum_{k=0}^{t-1} p^k a_k \quad \text{y} \quad b = \sum_{k=0}^{t-1} p^k b_k, \quad \text{con } a_k, b_k \in \mathbb{Z}_p, \text{ para } k = 0, 1, \ldots, t-1.$$

Puesto que $a + b, ab \in \mathbb{Z}_{p^t}$, tenemos que

$$a + b = \sum_{k=0}^{t-1} p^k u_k \quad \text{y} \quad ab = \sum_{k=0}^{t-1} p^k v_k, \quad \text{con } u_k, v_k \in \mathbb{Z}_p, \text{ para } k = 0, 1, \ldots, t-1.$$

Sin embargo, la expresión de los elementos u_k y v_k en términos de los elementos a_k, es una tarea delicada y su expresión muy compleja. Por ejemplo, para $t = 2$, de los lemas 2.1 y 2.2 tenemos que

$$a + b = p\left[\left(a_1 + b_1 + \left\lfloor \frac{a_0 + b_0}{p} \right\rfloor\right) \bmod p\right] + (a_0 + b_0) \bmod p,$$

$$ab = p\left[\left(a_0 b_1 + a_1 b_0 + \left\lfloor \frac{a_0 b_0}{p} \right\rfloor\right) \bmod p\right] + (a_0 b_0) \bmod p.$$

Es decir, necesitamos $a_0 + b_0$ y $a_0 b_0$ para calcular u_1 y v_1 respectivamente. Análogamente, para $t = 3$, tenemos que

$$a + b = p^2\left[\left(a_2 + b_2 + \left\lfloor \frac{a_1 + b_1 + \left\lfloor \frac{a_0 + b_0}{p} \right\rfloor}{p} \right\rfloor\right) \bmod p\right]$$
$$+ p\left[\left(a_1 + b_1 + \left\lfloor \frac{a_0 + b_0}{p} \right\rfloor\right) \bmod p\right] + (a_0 + b_0) \bmod p,$$

$$ab = p^2\left[\left(a_0 b_2 + a_1 b_1 + a_2 b_0 + \left\lfloor \frac{a_0 b_1 + a_1 b_0 + \left\lfloor \frac{a_0 b_0}{p} \right\rfloor}{p} \right\rfloor\right) \bmod p\right]$$
$$+ p\left[\left(a_0 b_1 + a_1 b_0 + \left\lfloor \frac{a_0 b_0}{p} \right\rfloor\right) \bmod p\right] + (a_0 b_0) \bmod p.$$

Notemos que, como en el caso anterior, necesitamos $a_0 + b_0$ y $a_0 b_0$ para calcular u_1 y v_1 respectivamente. Pero además, también necesitamos $a_0 + b_0$ y $a_1 + b_1$ para calcular u_2, y $a_0 b_1 + a_1 b_0$ y $a_0 b_0$ para calcular v_2. ■

A través de un proceso recursivo en el que utilizamos la observación 3.1, obtenemos el siguiente resultado que generaliza los lemas 2.1 y 2.2 demostrados en el capítulo 2.

Lema 3.1: *Supongamos que p es un número primo, que t es un entero positivo y que*

$$a = \sum_{k=0}^{t-1} p^k a_k \quad y \quad b = \sum_{k=0}^{t-1} p^k b_k \quad \text{con } a_k, b_k \in \mathbb{Z}_p, \text{ para } k = 0, 1, 2, \ldots, t-1.$$

(a) *Sumongamos además que $c_k = a_k + b_k$, para $k = 0, 1, 2, \ldots, t-1$. Sea $d_{-1} = 0$ y definamos d_k y u_k, para $k = 0, 1, 2, \ldots, t-1$, como*

$$d_k = c_k + \left\lfloor \frac{d_{k-1}}{p} \right\rfloor \qquad y \qquad u_k = d_k \bmod p.$$

Entonces $u_k \in \mathbb{Z}_p$ para $k = 0, 1, 2, \ldots, t-1$, y $a + b = \sum_{k=0}^{t-1} p^k u_k$.

(b) *Supongamos además que $e_k = \sum_{l=0}^{k} a_{k-l} b_l$, para $k = 0, 1, 2, \ldots, t-1$. Sea $f_{-1} = 0$ y definamos f_k y v_k, para $k = 0, 1, 2, \ldots, t-1$, como*

$$f_k = e_k + \left\lfloor \frac{f_{k-1}}{p} \right\rfloor \qquad y \qquad v_k = f_k \bmod p.$$

Entonces $v_k \in \mathbb{Z}_p$ para $k = 0, 1, 2, \ldots, t-1$, y $ab = \sum_{k=0}^{t-1} p^k v_k$.

DEMOSTRACIÓN: La demostración se realiza por inducción sobre t. Sabemos, por la observación 3.1, que el resultado es cierto para $t = 2, 3$.

Supongamos que el resultado es cierto para $t = n - 1$ y veamos que también lo es para $t = n$.

Si $a, b \in \mathbb{Z}_{p^n}$, entonces

$$a = \sum_{k=0}^{n-1} p^k a_k \quad \text{y} \quad b = \sum_{k=0}^{n-1} p^k b_k \quad \text{con } a_k, b_k \in \mathbb{Z}_p, \text{ para } k = 0, 1, 2, \ldots, n-1.$$

Puesto que $\sum_{k=0}^{n-2} p^k a_k, \sum_{k=0}^{n-2} p^k b_k \ \in \mathbb{Z}_{p^{n-1}}$, por la hipótesis de inducción tenemos que

$$\left(\sum_{k=0}^{n-2} p^k a_k\right) + \left(\sum_{k=0}^{n-2} p^k b_k\right) = \sum_{k=0}^{n-2} p^k u_k$$

donde, para $k = 0, 1, 2, \ldots, n-2$ es

$$u_k = d_k \bmod p,\ d_k = c_k + \left\lfloor \frac{d_{k-1}}{p} \right\rfloor,\ c_k = a_k + b_k$$

con $d_{-1} = 0$. Ahora, si

$$u_{n-1} = d_{n-1} \bmod p,\ d_{n-1} = c_{n-1} + \left\lfloor \frac{d_{n-2}}{p} \right\rfloor,\ c_{n-1} = a_{n-1} + b_{n-1}$$

tenemos que

$$\begin{aligned} a + b &= p^{n-1} a_{n-1} + \sum_{k=0}^{n-2} p^k a_k + p^{n-1} b_{n-1} + \sum_{k=0}^{n-2} p^k b_k \\ &= p^{n-1} \left(\left(a_{n-1} + b_{n-1} + \left\lfloor \frac{d_{n-2}}{p} \right\rfloor \right) \bmod p \right) + \sum_{k=0}^{n-2} p^k u_k \\ &= \sum_{k=0}^{n-1} p^k u_k. \end{aligned}$$

Mediante un razonamiento análogo podemos ver que

$$\left(\sum_{k=0}^{n-2} p^k a_k\right)\left(\sum_{k=0}^{n-2} p^k b_k\right) = \sum_{k=0}^{n-2} p^k v_k$$

donde, para $k = 0, 1, 2, \ldots, n-2$ es

$$v_k = f_k \bmod p,\ f_k = e_k + \left\lfloor \frac{f_{k-1}}{p} \right\rfloor,\ e_k = \sum_{l=0}^{k} p^{k-l} b_l$$

con $f_{-1} = 0$. Ahora, si

$$v_{n-1} = f_{n-1} \bmod p,\ f_{n-1} = e_{n-1} + \left\lfloor \frac{f_{n-2}}{p} \right\rfloor,\ e_{n-1} = \sum_{l=0}^{n-1} p^{n-1-l} b_l$$

tenemos que

$$\begin{aligned} ab &= \left(p^{n-1}a_{n-1} + \sum_{k=0}^{n-2} p^k a_k\right) + \left(p^{n-1}b_{n-1} + \sum_{k=0}^{n-2} p^k b_k\right) \\ &= \left(p^{n-1}\right)^2 a_{n-1}b_{n-1} + p^{n-1}a_{n-1}\left(\sum_{k=0}^{n-2} p^k b_k\right) \\ &+ \left(\sum_{k=0}^{n-2} p^k a_k\right) p^{n-1}b_{n-1} + \left(\sum_{k=0}^{n-2} p^k a_k\right)\left(\sum_{k=0}^{n-2} p^k b_k\right) \\ &= p^{n-1}\left(\left(\sum_{l=0}^{n-1} a_{n-l-1}b_l + \left\lfloor \frac{f_{n-2}}{p} \right\rfloor\right) \bmod p\right) + \sum_{k=0}^{n-2} p^k v_k \\ &= \sum_{k=0}^{n-1} p^k v_k. \end{aligned}$$

□

A continuación establecemos la condición necesaria y suficiente para que un elemento $a \in \mathbb{Z}_{p^t}$ sea invertible.

Lema 3.2: *Supongamos que p es un número y que t es un entero positivo. Entonces $a \in \mathbb{Z}_{p^t}$ es invertible si y sólo si $a \bmod p \neq 0$.*

DEMOSTRACIÓN: Recordemos que $a \in \mathbb{Z}_{p^t}$ es invertible si y sólo si $\mathrm{mcd}(a, p^t) = 1$. Ahora bien, como p es un número primo, sabemos que $\mathrm{mcd}(a, p) = 1$ si y sólo si $\mathrm{mcd}(a, p^l) = 1$, para todo entero positivo l. finalmente, como $\mathrm{mcd}(a, p) = 1$ si y sólo si $a \bmod p \neq 0$, concluimos que a es invertible si y sólo si $a \bmod p \neq 0$. □

La observación que sigue será útil en la sección 3.2.2..

Observación 3.2: Si t es un entero positivo y $a \in \mathbb{Z}_{p^t}$ es invertible, entonces, de acuerdo a la demostración del lema 3.2, tenemos que $\mathrm{mcd}(a, p^t) = 1$ y por la identidad de Bézout.

$$a\bar{a} + p^t q = 1, \quad \text{para algunos } \bar{a}, q \in \mathbb{Z}.$$

Por tanto, $a\bar{a} \equiv 1 \pmod{p^t}$. Además, puesto que $a\bar{a} + p^l(p^{t-l}q) = 1$, para $l = 1, 2, \ldots, t$, tenemos que

$$a\bar{a} \equiv 1 \pmod{p^l}, \quad \text{para } l = 1, 2, \ldots, t. \tag{3.2}$$

Supongamos ahora que

$$a = \sum_{k=0}^{t-1} p^k a_k, \quad \text{con } a_k \in \mathbb{Z}_p, \text{ para } k = 0, 1, 2, \ldots, t-1.$$

Obtener una expresión explicita para $\bar{a}$ en términos de los enteros a_k, para $k = 0, 1, \ldots, t-1$ no es una tarea fácil. Por ejemplo, para $t = 2$ se sigue del lema 2.3 que

$$\bar{a} = p\left[\left(-a_1\bar{a}_0^2 - \left\lfloor \frac{a_0\bar{a}_0}{p} \right\rfloor \bar{a}_0\right) \bmod p\right] + \bar{a}_0 \tag{3.3}$$

donde, de acuerdo a la expresión (3.2), $\bar{a}_0 \in \mathbb{Z}_p$ es el entero tal que

$$a_0\bar{a}_0 \equiv 1 \pmod{p}.$$

■

3.2 El anillo $E_p{}^{(m)}$

3.2.1 Caracterización del anillo $E_p{}^{(m)}$

Comenzamos con el siguiente resultado en el que introducimos el anillo $E_p{}^{(m)}$. Aquí, denotamos por $\mathrm{Mat}_m(\mathbb{Z})$ el conjunto de las matrices de tamaño $m \times m$ con elementos en $\mathbb{Z}$.

Teorema 3.1: *Supongamos que p es un número primo y que $m \geq 2$ es un entero. El conjunto*

$$E_p{}^{(m)} = \left\{[a_{ij}] \in \mathrm{Mat}_m(\mathbb{Z}) \mid a_{ij} \in \mathbb{Z}_{p^i} \text{ si } i \leq j,\ a_{ij} \in p^{i-j}\mathbb{Z}_{p^j} \text{ si } i > j\right\} \tag{3.4}$$

es un anillo unitario y no conmutativo con la adición y la multiplicación definidas, respectivamente, como

$$[a_{ij}] + [b_{ij}] = \left[(a_{ij} + b_{ij}) \bmod p^i\right], \tag{3.5}$$

$$[a_{ij}] \cdot [b_{ij}] = \left[\left(\sum_{k=1}^{m} a_{ik}b_{kj}\right) \bmod p^i\right]. \tag{3.6}$$

DEMOSTRACIÓN: Esta demostración es una simple comprobación del resultado. □

Notemos que la adición y la multiplicación de elementos de ${E_p}^{(m)}$ es análoga a la adición y la multilicación de matrices en $\mathrm{Mat}_m(\mathbb{Z})$, con la particularidad de que los elementos de la i-ésima fila se reducen módulo p^i, para $i = 1, 2, \ldots, m$.

Una consecuencia del resultado anterior es que la matriz nula y la matriz identidad son las identidades aditiva y multiplicativa de ${E_p}^{(m)}$ que denotamos por O e I, respectivamente. Además, si tenemos en cuenta cómo se calculan los opuestos en $\mathbb{Z}_{p^i}$, es evidente que el opuesto del elemento $[a_{ij}] \in {E_p}^{(m)}$ es $[p^i - a_{ij}] \in {E_p}^{(m)}$. Caracterizaremos los elementos invertibles de ${E_p}^{(m)}$ en la sección 3.2.2.

Notemos que $E_p^{(2)} = E_p$. Además, para $l = 2, 3, \ldots, m-1$, la aplicación $f_l : E_p^{(l)} \longrightarrow E_p^{(l+1)}$ dada por

$$f\left(\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1l} \\ a_{21} & a_{22} & \cdots & a_{2l} \\ \vdots & \vdots & & \vdots \\ a_{l1} & a_{l2} & \cdots & a_{ll} \end{bmatrix}\right) = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1l} & 0 \\ a_{21} & a_{22} & \cdots & a_{2l} & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ a_{l1} & a_{l2} & \cdots & a_{ll} & 0 \\ 0 & 0 & \cdots & 0 & 0 \end{bmatrix}$$

es un monomorfismo de anillos, lo cual nos permite embeber el anillo $E_p^{(l)}$ en el anillo $E_p^{(l+1)}$ y, por tanto, podemos considerar que $E_p^{(l)}$ es un subanillo de $E_p^{(l+1)}$. En consecuencia, tenemos la siguiente cadena de anillos

$$E_p^{(2)} \subset E_p^{(3)} \subset \cdots \subset E_p^{(m-1)} \subset E_p^{(m)}$$

y, por tanto, $E_p^{(l)}$, para $l = 3, 4, \ldots, m$, es un anillo semilocal que no se puede embeber en ningún anillo de matrices sobre un anillo conmutativo.

Terminamos esta sección con el siguiente resultado en el que establecemos el número de elementos de ${E_p}^{(m)}$, en función de p y m.

Teorema 3.2: *Supongamos que p es un número primo y que $m \geq 2$ es un entero. Entonces* $\mathrm{Card}\left({E_p}^{(m)}\right) = p^{\nu_m}$ *donde*

$$\nu_m = \frac{2m^3 + 3m^2 + m}{6}. \tag{3.7}$$

DEMOSTRACIÓN: Procedemos por inducción sobre m. Para $m = 2$, sabemos que $\text{Card}\,(E_p) = p^5$ y $\nu_2 = 5$, como consecuencia de los teoremas 2.1 y 2.5.

Supongamos que $\text{Card}\left(E_p{}^{(m-1)}\right) = p^{\nu_{m-1}}$ y consideremos un elemento $A \in E_p{}^{(m)}$. Es evidente que podemos escribir A como

$$A = \left[\begin{array}{ccccc|c} & & & & & a_{1m} \\ & & & & & a_{2m} \\ & & & \bar{A} & & \vdots \\ & & & & & a_{(m-1)m} \\ \hline a_{m1} & a_{m2} & \cdots & & a_{m(m-1)} & a_{mm} \end{array}\right], \quad \text{con } \bar{A} \in E_p^{(m-1)}.$$

Recordemos que de la expresión (3.4) tenemos que $a_{im} \in \mathbb{Z}_{p^i}$ para $i = 1, 2, \ldots, m$ y que $a_{mj} \in p^{m-j}\mathbb{Z}_{p^j}$, para $j = 1, 2, \ldots, m-1$. Así, una vez fijado el elemento $\bar{A}$, tenemos

$$p \cdot p^2 \cdots p^{m-1} \cdot p^m \cdot p \cdot p^2 \cdots p^{m-1} = p^{m^2}$$

formas diferentes de elegir A. Por tanto, $\text{Card}\left(E_p{}^{(m)}\right) = p^{\nu_{m-1}} p^{m^2}$.

Ahora, es fácil comprobar que $\nu_{m-1} + m^2 = \nu_m$, con lo cual tenemos que

$$\text{Card}\left(E_p{}^{(m)}\right) = p^{\nu_m}. \qquad \square$$

3.2.2 Elementos invertibles

En esta sección caracterizamos los elementos invertibles de $E_p{}^{(m)}$ y calculamos su número. Antes, sin embargo, introducimos una serie de lemas que nos permitirán obtener dicha caracterización de una forma sencilla. Supondremos, como viene siendo habitual, que p es un número primo y $m \geq 2$ un entero.

Lema 3.3: *Consideremos el elemento*

$$A = \begin{bmatrix} a_1 & 0 & \cdots & 0 \\ 0 & a_2 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & a_m \end{bmatrix} \in E_p^{(m)}.$$

Si $a_i \bmod p \neq 0$, para $i = 1, 2, \ldots, m$, entonces A es invertible en ${E_p}^{(m)}$ y, en tal caso

$$A^{-1} = \begin{bmatrix} \bar{a}_1 & 0 & \cdots & 0 \\ 0 & \bar{a}_2 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & \bar{a}_m \end{bmatrix}$$

donde, de acuerdo con la expresión (3.2), $\bar{a}_i \in \mathbb{Z}_{p^i}$ es el entero tal que

$$a_i \bar{a}_i \equiv 1 \pmod{p^i}, \quad \text{para} \quad i = 1, 2, \ldots, m.$$

DEMOSTRACIÓN: La demostración consiste en la simple comprobación del resultado. □

Lema 3.4: *Supongamos que $A, B \in E_p^{(m)}$ con*

$$A = \begin{bmatrix} 1 & 0 & \cdots & 0 & a_{1m} \\ 0 & 1 & \cdots & 0 & a_{2m} \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & a_{(m-1)m} \\ 0 & 0 & \cdots & 0 & 1 \end{bmatrix} \quad y \quad B = \begin{bmatrix} 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \\ b_{m1} & b_{m2} & \cdots & b_{m(m-1)} & 1 \end{bmatrix}.$$

Entonces A y B son invertibles en $E_p^{(m)}$ y

$$A^{-1} = \begin{bmatrix} 1 & 0 & \cdots & 0 & -a_{1m} \\ 0 & 1 & \cdots & 0 & -a_{2m} \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -a_{(m-1)m} \\ 0 & 0 & \cdots & 0 & 1 \end{bmatrix}, B^{-1} = \begin{bmatrix} 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \\ -b_{m1} & -b_{m2} & \cdots & -b_{m(m-1)} & 1 \end{bmatrix} \tag{3.8}$$

son los correspondientes inversos.

DEMOSTRACIÓN: La demostración es directa. Sean M y N las matrices de los segundos miembros, respectivamente, en la última expresión. Es fácil comprobar que

$AM = I = MA$ y $BN = I = NB$, por tanto, A y B son invertibles en $E_p{}^{(m)}$ y $A^{-1} = M$ y $B^{-1} = N$. □

Con el fin de caracterizar los elementos invertibles de $E_p{}^{(m)}$, notemos que si $A = [a_{ij}] \in E_p{}^{(m)}$, entonces de la expresión (3.4) tenemos que

$$a_{ij} = \begin{cases} \displaystyle\sum_{r=1}^{i} p^{i-r} a_{ij}^{(i-r)}, \text{ con } a_{ij}^{(i-r)} \in \mathbb{Z}_p, & \text{si } i \leq j, \\ \displaystyle p^{i-j} \left(\sum_{r=1}^{j} p^{j-r} a_{ij}^{(j-r)} \right), \text{ con } a_{ij}^{(j-r)} \in \mathbb{Z}_p, & \text{si } i > j. \end{cases} \tag{3.9}$$

Lema 3.5: *Sea $A = [a_{ij}] \in E_p{}^{(m)}$ tal que $a_{mm} \bmod p \neq 0$. Para $i, j = 1, 2, \ldots, m-1$ consideremos el entero a_{ij}^* definido como*

$$a_{ij}^* = (a_{ij} - a_{im}\bar{a}_{mm}a_{mj}) \bmod p^i, \tag{3.10}$$

donde, de acuerdo con la expresión (3.2), $\bar{a}_{mm}$ es el entero tal que

$$a_{mm}\bar{a}_{mm} \equiv 1 \pmod{p^m}.$$

Entonces

(a) $a_{ij}^* = a_{ij}$, *para* $i = 1, 2, \ldots, m-1$ *y* $j = 1, 2, \ldots, m-i$,

(b) $a_{ij}^* \in p^{i-j}\mathbb{Z}_{p^j}$ *para* $i = \left\lfloor \frac{m+1}{2} \right\rfloor + 1, \left\lfloor \frac{m+1}{2} \right\rfloor + 2, \ldots, m-1$ *y* $j = m-i+1, m-i+2, \ldots, i-1$,

(c) $a_{ii}^* \bmod p = a_{ii} \bmod p$, *para* $i = \left\lfloor \frac{m+1}{2} \right\rfloor, \left\lfloor \frac{m+1}{2} \right\rfloor + 1, \ldots, m-1$.

Demostración: Es evidente que $a_{ij}^* \in \mathbb{Z}_{p^i}$, para $i = 1, 2, \ldots, m-1$ and $j = 1, 2, \ldots, m-1$.

Las propiedades (a), (b) y (c) se obtienen a partir de la expresión (3.10) y el lema 3.1, después de realizar las manipulaciones algebraicas oportunas. □

Notemos que con la notación del lema anterior, $A^* = \left[a_{ij}^*\right] \in E_p{}^{(m)}$.

Lema 3.6: *Sea* $A = [a_{ij}] \in {E_p}^{(m)}$ *tal que* $a_{mm} \bmod p \neq 0$. *Entonces con la notación del lema 3.5, tenemos que*

$$A = \begin{bmatrix} 1 & 0 & \cdots & 0 & a_{1m}\bar{a}_{mm} \\ 0 & 1 & \cdots & 0 & a_{2m}\bar{a}_{mm} \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & a_{(m-1)m}\bar{a}_{mm} \\ 0 & 0 & \cdots & 0 & 1 \end{bmatrix} \times$$

$$\begin{bmatrix} & & & & 0 \\ & & & & 0 \\ & & A^* & & \vdots \\ & & & & 0 \\ 0 & 0 & \cdots & 0 & a_{mm} \end{bmatrix} \begin{bmatrix} 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \\ \bar{a}_{mm}a_{m1} & \bar{a}_{mm}a_{m2} & \cdots & \bar{a}_{mm}a_{m(m-1)} & 1 \end{bmatrix}. \qquad (3.11)$$

Demostración: Supongamos que $i = 1, 2, \ldots, m-1$ y $j = 1, 2, \ldots, m-1$. Un cálculo directo muestra que el elemento que ocupa la posición (i, j) en la matriz del segundo miembro es $(a^*_{ij} + a_{im}\bar{a}_{mm}a_{mj}) \bmod p^i$; dicho elemento, por la expresión (3.10), es igual a a_{ij}.

De forma análoga, si $j = 1, 2, \ldots, m-1$, el elemento de la posición (m, j) en la matriz del segundo miembro es $(a_{mm}\bar{a}_{mm}a_{mj}) \bmod p^m$ que, por ser $a_{mm}\bar{a}_{mm} \equiv 1 \pmod{p^m}$, es igual a a_{mj}.

Por último, mediante un razonamiento similar, si $i = 1, 2, \ldots, m-1$, el elemento que ocupa la posición (i, m) en la matriz del segundo miembro, es a_{im}.

En consecuencia, se satisface la expresión (3.11). □

Nuestro siguiente resultado caracteriza los elementos invertibles de ${E_p}^{(m)}$. Sin embargo, antes de ello, introducimos la siguiente observación que será útil para la demostración de dicho resultado.

Observación 3.3: De acuerdo con la expresión (3.9) y el teorema 2.7, si

$$A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} = \begin{bmatrix} a^{(0)}_{11} & a^{(0)}_{12} \\ pa^{(0)}_{21} & pa^{(1)}_{22} + a^{(0)}_{22} \end{bmatrix} \in E^{(2)}_p$$

es invertible, entonces $a_{11}^{(0)} \neq 0$, $a_{22}^{(0)} \neq 0$, y

$$A^{-1} = \begin{bmatrix} b_{11}^{(0)} & b_{12}^{(0)} \\ pb_{21}^{(0)} & pb_{22}^{(1)} + b_{22}^{(0)} \end{bmatrix}$$

es el inverso de A con

$$\begin{aligned}
b_{11}^{(0)} &= \bar{a}_{11}^{(0)}, \\
b_{12}^{(0)} &= \left(-\bar{a}_{11}^{(0)} a_{12}^{(0)} \bar{a}_{22}^{(0)}\right) \bmod p, \\
b_{21}^{(0)} &= \left(-\bar{a}_{22}^{(0)} a_{21}^{(0)} \bar{a}_{11}^{(0)}\right) \bmod p, \\
b_{22}^{(1)} &= \left(a_{21}^{(0)} \bar{a}_{11}^{(0)} a_{12}^{(0)} \left(\bar{a}_{22}^{(0)}\right)^2 - a_{22}^{(1)} \left(\bar{a}_{22}^{(0)}\right)^2 - \left\lfloor \frac{a_{22}^{(0)} \bar{a}_{22}^{(0)}}{p} \right\rfloor \bar{a}_{22}^{(0)}\right) \bmod p, \\
b_{22}^{(0)} &= \bar{a}_{22}^{(0)},
\end{aligned}$$

donde, de acuerdo con la expresión (3.2), $\bar{a}_{ii}^{(0)}$ denota el elemento de $\mathbb{Z}_p$ tal que $a_{ii}^{(0)} \bar{a}_{ii}^{(0)} \equiv 1 \pmod{p}$, con $i = 1, 2$.

Además, de los lemas 3.3, 3.4, 3.5 y 3.6, tenemos que

$$\begin{aligned}
A^{-1} &= \begin{bmatrix} 1 & 0 \\ (-\bar{a}_{22} a_{21}) \bmod p^2 & 1 \end{bmatrix} \begin{bmatrix} \bar{a}_{11} & 0 \\ 0 & \bar{a}_{22} \end{bmatrix} \begin{bmatrix} 1 & (-a_{12}\bar{a}_{22}) \bmod p \\ 0 & 1 \end{bmatrix} \\
&= \begin{bmatrix} \bar{a}_{11} & (-\bar{a}_{11} a_{12} \bar{a}_{22}) \bmod p \\ (-\bar{a}_{22} a_{21} \bar{a}_{11}) \bmod p^2 & (\bar{a}_{22} a_{21} \bar{a}_{11} a_{12} \bar{a}_{22}) \bmod p^2 \end{bmatrix}
\end{aligned}$$

y, de acuerdo con las expresiones (3.9) and (3.3) tenemos que

$$\begin{aligned}
b_{11}^{(0)} &= \bar{a}_{11}, \\
b_{12}^{(0)} &= (-\bar{a}_{11} a_{12} \bar{a}_{22}) \bmod p, \\
pb_{21}^{(0)} &= (-\bar{a}_{22} a_{21} \bar{a}_{11}) \bmod p^2, \\
pb_{22}^{(1)} + b_{22}^{(0)} &= (\bar{a}_{22} a_{21} \bar{a}_{11} a_{12} \bar{a}_{22}) \bmod p^2.
\end{aligned}$$

■

Teorema 3.3: *Consideremos $A = [a_{ij}] \in {E_p}^{(m)}$. Entonces A es invertible si y sólo si $a_{ii} \bmod p \neq 0$ para $i = 1, 2, \ldots, m$.*

DEMOSTRACIÓN: Notemos que, de acuerdo con la expresión (3.9), $a_{ii} \bmod p = a_{ii}^{(0)}$, para $i = 1, 2, \ldots, m$.

Supongamos que A es invertible. Entonces existe $B = [b_{ij}] \in E_p^{(m)}$ tal que $AB = I$. Ahora bien, de las expresiones (3.6) y (3.9) no es difícil probar –aunque es algo tedioso – que $\left(a_{ii}^{(0)} b_{ii}^{(0)}\right) \bmod p = 1$, para $i = 1, 2, \ldots, m$, y por tanto, $a_{ii}^{(0)} \neq 0$, para $i = 1, 2, \ldots, m$. Recíprocamente, supongamos ahora que $a_{ii}^{(0)} \neq 0$, para $i = 1, 2, \ldots, m$.

Procedemos por inducción sobre m.

Para $m = 2$ el resultado se sigue del teorema 2.7 (ver además la observación 3.3). Supongamos pues que el resultado es cierto para $m - 1$; probemos que también lo es para m.

Puesto que $a_{mm}^{(0)} \neq 0$, por el lema 3.5 tenemos que $A^* = \left[a_{ij}^*\right] \in E_p^{(m-1)}$ y $a_{ii}^* \bmod p = a_{ii}^{(0)}$, para $i = 1, 2, \ldots, m-1$; de esta forma, $a_{ii}^* \bmod p \neq 0$, y por la hipótesis de inducción, A^* es invertible. Ahora, no es difícil probar que

$$\begin{bmatrix} & & & 0 \\ & A^* & & 0 \\ & & & \vdots \\ & & & 0 \\ 0 & 0 \cdots & 0 & a_{mm} \end{bmatrix}$$

es invertible y, por los lemas 3.6 y 3.4, A es invertible. □

Una vez caracterizados los elementos invertibles, ya estamos en condiciones de obtener el número de elementos invertibles de ${E_p}^{(m)}$.

Corolario 3.1: *El número de elementos invertibles de ${E_p}^{(m)}$ es $p^{\nu_m - m}(p-1)^m$ donde ν_m está definido en la expresión (3.7).*

DEMOSTRACIÓN: Supngamos que $A = [a_{ij}] \in E_p{}^{(m)}$ es invertible. Por el teorema 3.3, $a_{ii} \bmod p \neq 0$, para $i = 1, 2, \ldots, m$, lo cual es equivalente a decir que $\text{mcd}(a_{ii}, p^i) = 1$. Entonces, tenemos

$$pp^2 \cdots p^{i-1}\varphi(p^i)\overbrace{p^i p^i \cdots p^i}^{m-i} = p^{\mu_m(i)}(p-1)$$

maneras diferentes de elegir la i-ésima columna de A, donde, $\varphi(p^i) = p^{i-1}(p-1)$ y $\mu_m(i) = \dfrac{2im - i^2 - 1}{2}$. En consecuencia, el número de elementos invertibles es

$$\prod_{i=1}^{m} p^{\mu_m(i)}(p-1) = p^{\sum_{i=1}^{m}\mu_m(i)}(p-1)^m.$$

Ahora, es fácil probar que $\sum_{i=1}^{m}\mu_m(i) = \nu_m - m$, lo que completa la demostración.□

Como consecuencia del teorema 3.1 y del corolario 3.1, la fracción de elementos invertibles en $E_p{}^{(m)}$ es

$$\left(\frac{p-1}{p}\right)^m. \tag{3.12}$$

Por tanto, el número de elementos invertibles depende tanto de p elegido como de m.

Notemos que para un m fijo, si p es suficientemente grande, la expresión (3.12) tiende a 1 y, por tanto, la mayoría de los elementos de $E_p{}^{(m)}$ serían invertibles. Es lo que ocurre para $m = 2$ tal como vimos en la sección 2.3.2 para el caso de E_p. Sin embargo, si consideramos p y q primos tales que $p < q \leq m$, tenemos que

$$\left(\frac{p-1}{p}\right)^m < \left(\frac{q-1}{q}\right)^m \leq \left(\frac{m-1}{m}\right)^m \leq \frac{1}{e} \approx 0{,}3678.$$

Por tanto, cuanto menor sea el primo p en comparación con el entero m, menor será la proporción de elementos invertibles de $E_p{}^{(m)}$. En particular, para $p = m$ el número de elementos invertibles de $E_p{}^{(m)}$ representa menos del 37 % sobre el total de elementos.

La tabla 3.1 muestra el porcentaje de elementos invertibles de $E_p^{(32)}$ para distintos valores de p con $p \leq 32$. Análogamente, la tabla 3.2 muestra el porcentaje de elementos invertibles de $E_2^{(m)}$ para distinto valores de $m \geq 2$.

p	Elementos en ${E_p}^{(32)}$	% Elementos invertibles	% Elementos no invertibles
2	$2^{11440} \approx 6,07 \cdot 10^{3443}$	$2,3283064365 \cdot 10^{-8}$	99,9999999767
3	$3^{11440} \approx 1,85 \cdot 10^{5458}$	$2,3178200226 \cdot 10^{-4}$	99,9999976822
5	$5^{11440} \approx 1,65 \cdot 10^{7996}$	$0,0792281625$	$99,9207718375$
7	$7^{11440} \approx 8,35 \cdot 10^{9667}$	$0,7206140606$	$99,2793859394$
⋮	⋮	⋮	⋮
23	$23^{11440} \approx 1,47 \cdot 10^{15578}$	$24,1120998682$	$75,8879001318$
29	$29^{11440} \approx 6,81 \cdot 10^{16729}$	$32,5327720496$	$67,4672279504$
31	$31^{11440} \approx 1,51 \cdot 10^{17061}$	$35,0191780480$	$64,9808219520$

Tabla 3.1: *Porcentaje de elementos invertibles de $E_p^{(32)}$ para distintos valores de p.*

m	Elementos en ${E_2}^{(m)}$	% Elementos invertibles	% Elementos no invertibles
2	$2^5 = 32$	25	75
3	$2^{14} = 16384$	$12,5$	$87,5$
4	$2^{30} = 1073741824$	$6,25$	$93,75$
5	$2^{55} \approx 3,60 \cdot 10^{16}$	$3,125$	$96,875$
⋮	⋮	⋮	⋮
14	$2^{1015} \approx 3,51 \cdot 10^{305}$	$0,0061035156$	$99,993896484$
15	$2^{1240} \approx 1,89 \cdot 10^{373}$	$0,0030517578$	$99,996948242$
⋮	⋮	⋮	⋮
20	$2^{2870} \approx 9,04 \cdot 10^{863}$	$0,0000953674$	$99,999904633$

Tabla 3.2: *Porcentaje de elementos invertibles de $E_2^{(m)}$ para distintos valores de m.*

3.2.3 Otras propiedades

En esta sección recogemos algunas propiedades de ${E_p}^{(m)}$ que utilizaremos en el capítulo siguiente.

Lema 3.7: *El centro de* $E_p{}^{(m)}$ *es el conjunto*

$$Z\left(E_p{}^{(m)}\right) = \left\{ [a_{ij}] \in \mathrm{Mat}_m(\mathbb{Z}) \mid a_{ii} = \sum_{j=0}^{i-1} p^j x_j, \text{ con } x_j \in \mathbb{Z}_p \text{ y } a_{ij} = 0 \text{ si } i \neq j \right\}.$$

y, en consecuencia, $\mathrm{Card}\left(Z\left(E_p{}^{(m)}\right)\right) = p^m$.

Demostración: La demostración sigue un razonamiento análogo al utilizado en la demostración del teorema 2.9 para $Z\left(E_p{}^{(m)}\right)$. □

Notemos que como consecuencia de los teoremas 2.9 y 3.7 y la cadena de inclusiones de la expresión 3.1 tenemos que

$$Z\left(E_p^{(2)}\right) \subseteq Z\left(E_p^{(3)}\right) \subseteq \ldots \subseteq Z\left(E_p^{(m-1)}\right) \subseteq Z\left(E_p^{(m)}\right).$$

Por tanto, de acuerdo con los comentarios del final de la sección 2.3.3 tenemos que tanto $Z\left(E_p{}^{(m)}\right)$ como $E_p{}^{(m)}$ tienen divisores de cero y, en consecuencia, ni $Z\left(E_p{}^{(m)}\right)$ ni $E_p{}^{(m)}$ son dominios de integridad ni pueden ser, por tanto, anillos euclidianos.

Capítulo 4

Intercambios de claves y esquemas de multidifusión sobre anillos no conmutativos

4.1 Introducción

Como comentamos en la sección 1.1, desde que Diffie y Hellman [22] propusieron el primer algoritmo de intercambio de claves, han sido muchos los autores que han abordado dicho problema como pone de manifiesto la extensa bibliografía existente sobre el mismo. Véase, por ejemplo, [5, 18, 32, 39, 47, 48, 53].

La mayoría de los algoritmos propuestos hasta la fecha están relacionados con las propiedades de las operaciones sobre estructuras algebraicas conmutativas y muchos de los ataques más eficientes conocidos se basan precisamente en la conmutatividad de dichas estructuras. Como consecuencia de ello, existe una gran actividad orientada al desarrollo de nuevos criptosistemas y protocolos de intercambio de claves basados en estructuras no conmutativas.

El objetivo de este capítulo es el desarrollo de algunos protocolos de intercambio de claves y esquemas de multidifusión de claves sobre anillos no conmutativos, así como el estudio de su seguridad cuando son definidos sobre los anillos E_p y ${E_p}^{(m)}$ introducidos en los capítulos 2 y 3, respectivamente.

4.2 Intercambios de claves

4.2.1 Protocolos de intercambio de claves

Stickel [56] introduce en 2005 un protocolo de intercambio de claves para el cual utiliza el grupo $G = \langle C^a S, TD^b \rangle$, generado por las matrices $C^a S$ y TD^b, donde C y D son las matrices asociadas a dos polinomios irreducibles $p(\mathsf{X})$ y $q(\mathsf{X})$, respectivamente, de grado n sobre $\mathbb{F}_2$ (el cuerpo de Galois con dos elementos). S y T son dos matrices invertibles en una extensión del cuerpo $\mathbb{F}_2$ para las cuales SCS^{-1} y TDT^{-1} son matrices diagonales, cuyos elementos de la diagonal son las raíces de $p(\mathsf{X})$ y $q(\mathsf{X})$, respectivamente, en la extensión del cuerpo $\mathbb{F}_2$ y a y b son dos enteros cualesquiera.

A partir del intercambio de claves introducido por Stickel [56], proponemos el siguiente intercambio de claves sobre un anillo no conmutativo R.

Protocolo 4.1: *Suponemos que los elementos M, $N \in R$ son públicos.*

Paso 1: *Alicia y Bernardo eligen sus claves privadas $(r, s), (u, v) \in \mathbb{N}^2$ respectivamente.*

Paso 2: *Alicia calcula su clave pública $P_A = M^r N M^s$ y se la envía a Bernardo. De forma análoga, Bernardo calcula su clave pública $P_B = M^u N M^v$ y se la envía a Alicia.*

Paso 3: *Alicia y Bernardo calculan S_A y S_B, respectivamente, como*

$$S_A = M^r P_B M^s \quad y \quad S_B = M^u P_A M^v.$$

El secreto compartido es $S_A = S_B$, como ponemos de manifiesto en el teorema siguiente.

Teorema 4.1: *Con la notación del protocolo 4.1, tenemos que $S_A = S_B$.*

DEMOSTRACIÓN: Basta tener en cuenta que $M^k M^l = M^l M^k$, para todo $k, l \in \mathbb{N}$.

Notemos que si $MN = NM$, tenemos que

$$P_A = M^r N M^s = N M^r M^s \quad \text{y} \quad P_B = M^u N M^v = N M^u M^v,$$

entonces

$$NS_A = N M^r M^u N M^v M^s = M^r N M^s M^u N M^v = P_A P_B,$$
$$NS_B = N M^u M^r N M^s M^v = M^u N M^v M^r N M^s = P_B P_A.$$

Es inmediato observar que $P_A P_B = P_B P_A$ y, por tanto, que $NS_A = NS_B$, de forma que el secreto compartido, $S_A = S_B$, es fácilmente obtenido por alguien no autorizado debido a que los elementos N, P_A y P_B son públicos.

En consecuencia, necesitamos que $MN \neq NM$; por tanto, a partir de ahora supondremos que $N \notin Z(R)$, de modo que la seguridad de este protocolo se basa en la elección de un elemento M con un orden elevado. Sin embargo, si utilizamos las ideas de Shpilrain [51] es fácil criptoanalizar el protocolo anterior debido a que el elemento M es público. Si un atacante encuentra dos elementos $X, Y \in R$ tales que

$$XM = MX, \quad YM = MY \quad \text{y} \quad P_A = XNY,$$

entonces puede calcular

$$XP_B Y = XM^u N M^v Y = M^u P_A M^v = S_B,$$

de forma que obtiene el secreto compartido.

Para evitar esta debilidad proponemos dos nuevos protocolos de intercambio de claves, donde consideramos los elementos $f(M)$ y $g(M)$, obtenidos a partir de un elemento $M \in R$ y dos polinomios $f(\mathsf{X}), g(\mathsf{X}) \in Z(R)[\mathsf{X}]$.

Notemos que si $k, l \in \mathbb{N}$, aunque R es un anillo no conmutativo, tenemos que

$$f(M)^k g(M)^l = g(M)^l f(M)^k, \text{ para todo } M \in R. \tag{4.1}$$

Esta propiedad es la idea central que nos permite definir los siguientes protocolos de intercambio de claves.

En el primero de los protocolos que proponemos cada uno de los usuarios elige para su clave secreta un único polinómio con coeficientes en el centro del anillo y dos esteros positivos, como mostramos a continuación.

Protocolo 4.2: *Supongamos que los elementos $M \in R$ y $N \in R \setminus Z(R)$ son públicos.*

Paso 1: *Alicia elige su clave privada $f(\mathsf{X}) \in Z(R)[\mathsf{X}]$ y $(r,s) \in \mathbb{N}^2$.*
Bernardo, elige su clave privada $g(\mathsf{X}) \in Z(R)[\mathsf{X}]$ y $(u,v) \in \mathbb{N}^2$.

Paso 2: *Alicia calcula su clave pública $P_A = f(M)^r N f(M)^s$, y se la envía a Bernardo.*
Análogamente, Bernardo calcula su clave pública $P_B = g(M)^u N g(M)^v$, y se la envía a Alicia.

Paso 3: *Alicia y Bernardo calculan S_A y S_B, respectivamente, como*

$$S_A = f(M)^r P_B f(M)^s \quad y \quad S_B = g(M)^u P_A g(M)^v.$$

El secreto compartido es $S_A = S_B$, tal y como establece en el teorema que sigue.

Teorema 4.2: *Con la notación del protocolo 4.2, tenemos que $S_A = S_B$.*

DEMOSTRACIÓN: La demostración es consecuencia inmediata de la expresión (4.1).□

El ejemplo que desarrollamos a continuación nos permite mostrar el funcionamiento del protocolo propuesto sobre el anillo E_p estudiado en el capítulo 2. Con objeto de simplificar los cálculos y la presentación, consideramos un valor pequeño de p, concretamente $p = 31$, aunque hay que tener en cuenta que para la implementación práctica del protocolo debemos considerar valores de p del orden de 60 cifras decimales.

Ejemplo 4.1: Para iniciar el protocolo 4.2, consideramos públicos los elementos

$$M = \begin{bmatrix} 19 & 22 \\ 62 & 893 \end{bmatrix} \in E_{31} \quad \text{y} \quad N = \begin{bmatrix} 22 & 27 \\ 775 & 521 \end{bmatrix} \in E_{31} \setminus Z(E_{31}).$$

Los pasos del protocolo son:

Paso 1: Alicia elige su clave privada formada por los enteros $(r,s) = (5,7)$ y el

polimomio $f(\mathsf{X}) \in Z\left(E_{31}\right)[\mathsf{X}]$, dado por la expresión

$$f(\mathsf{X}) = \begin{bmatrix} 15 & 0 \\ 0 & 77 \end{bmatrix} + \begin{bmatrix} 2 & 0 \\ 0 & 777 \end{bmatrix} \mathsf{X}^2 + \begin{bmatrix} 17 & 0 \\ 0 & 482 \end{bmatrix} \mathsf{X}^4,$$

con lo que calcula

$$f(M) = \begin{bmatrix} 4 & 13 \\ 124 & 295 \end{bmatrix}.$$

Bernardo elige su clave privada formada por los enteros $(u, v) = (9, 8)$ y el polinomio $g(\mathsf{X}) \in Z\left(E_{31}\right)[\mathsf{X}]$, dado por la expresión

$$g(\mathsf{X}) = \begin{bmatrix} 7 & 0 \\ 0 & 472 \end{bmatrix} \mathsf{X} + \begin{bmatrix} 12 & 0 \\ 0 & 508 \end{bmatrix} \mathsf{X}^2 + \begin{bmatrix} 1 & 0 \\ 0 & 869 \end{bmatrix} \mathsf{X}^6,$$

y calcula

$$g(M) = \begin{bmatrix} 3 & 7 \\ 806 & 50 \end{bmatrix}.$$

Paso 2: Alicia calcula su clave pública P_A como

$$P_A = f(M)^r N f(M)^s = \begin{bmatrix} 11 & 15 \\ 403 & 355 \end{bmatrix},$$

y se la envía a Bernardo.

De forma similar, Bernardo calcula su clave pública P_B como

$$P_B = g(M)^u N g(M)^v = \begin{bmatrix} 19 & 29 \\ 558 & 562 \end{bmatrix},$$

y se la envía a Alicia.

Paso 3: Alicia calcula S_A como

$$S_A = f(M)^r P_B f(M)^s = \begin{bmatrix} 25 & 26 \\ 589 & 714 \end{bmatrix}.$$

Bernardo calcula S_B como

$$S_B = g(M)^u P_A g(M)^v = \begin{bmatrix} 25 & 26 \\ 589 & 714 \end{bmatrix}.$$

Como consecuencia del teorema 4.2, el secreto compartido es $S_A = S_B$.

Notemos que un atacante conoce el elemento M, ya que es público, pero los elementos $f(\mathsf{X}), g(\mathsf{X}) \in Z\left(E_{31}\right)[\mathsf{X}]$ son desconocidos. Por tanto, los siguientes elementos son también desconocidos

$$f(M)^r = \begin{bmatrix} 4 & 13 \\ 124 & 295 \end{bmatrix}^5 = \begin{bmatrix} 1 & 0 \\ 0 & 94 \end{bmatrix} \quad \text{y} \quad f(M)^s = \begin{bmatrix} 4 & 13 \\ 124 & 295 \end{bmatrix}^7 = \begin{bmatrix} 16 & 12 \\ 558 & 8 \end{bmatrix},$$

así como

$$g(M)^u = \begin{bmatrix} 3 & 7 \\ 806 & 50 \end{bmatrix}^9 = \begin{bmatrix} 29 & 4 \\ 186 & 295 \end{bmatrix} \quad \text{y} \quad g(M)^v = \begin{bmatrix} 3 & 7 \\ 806 & 50 \end{bmatrix}^8 = \begin{bmatrix} 20 & 1 \\ 527 & 9 \end{bmatrix}.$$

Supongamos que un atacante intercepta P_A y P_B. En primer lugar, para obtener el secreto compartido, el atacante debe determinar los polinomios $f(\mathsf{X})$ y $g(\mathsf{X})$ para, posteriormente, obtener los pares (r, s) y (u, v) a partir de las expresiones

$$f(M)^r N f(M)^s = P_A \quad \text{y} \quad g(M)^u N g(M)^v = P_B.$$

Esto es equivalente a resolver dos problemas de tipo DP, debido a que (r, s) y (u, v) son desconocidos. ■

Es posible proponer un ataque por fuerza bruta sobre el conjunto de polinomios con coeficientes en el centro del anillo. Sin embargo, un ataque de este tipo no es viable debido a que el número de polinomios de grado n con coeficientes en el centro de E_p es exactamente $(n+1)p^2$ (recordemos que $\text{Card}\left(Z\left(E_p\right)\right) = p^2$). Por tanto, basta tomar un primo p suficientemente grande o un valor de n para los polinomios lo suficientemente elevado.

A modo orientativo, si consideramos un primo p de alrededor de 60 cifras decimales y polinomios de grado $n = 20$, requisitos que no son demasiado exigentes a nivel computacional, el número de polinomios total es del orden de 10^{121}, lo que

E_p	Grado del polinomio									
p \ n	2	3	4	5	$\cdots$	12	13	$\cdots$	20	$\cdots$
2	12	16	20	24	$\cdots$	52	56	$\cdots$	84	$\cdots$
3	27	36	45	54	$\cdots$	117	126	$\cdots$	189	$\cdots$
5	75	100	125	150	$\cdots$	325	350	$\cdots$	525	$\cdots$
7	147	196	245	294	$\cdots$	637	686	$\cdots$	1029	$\cdots$
11	363	484	605	726	$\cdots$	1573	1694	$\cdots$	2541	$\cdots$
13	507	676	845	1014	$\cdots$	2197	2366	$\cdots$	3549	$\cdots$
17	867	1156	1445	1731	$\cdots$	3757	4046	$\cdots$	6069	$\cdots$
19	1083	1444	1805	2166	$\cdots$	4693	5054	$\cdots$	7581	$\cdots$
23	1587	2116	2645	3174	$\cdots$	6877	7406	$\cdots$	11109	$\cdots$
29	2523	3364	4205	5046	$\cdots$	10933	11774	$\cdots$	17661	$\cdots$
31	2883	3844	4805	5766	$\cdots$	12493	13454	$\cdots$	20181	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$		$\vdots$	$\vdots$		$\vdots$	
97	28227	37636	47045	56454	$\cdots$	122317	131726	$\cdots$	197589	$\cdots$
101	30603	40804	51005	61206	$\cdots$	132613	142814	$\cdots$	214221	$\cdots$
103	31827	42436	53045	63654	$\cdots$	137917	148526	$\cdots$	222789	$\cdots$
107	34347	45796	57245	68694	$\cdots$	148837	160286	$\cdots$	240429	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$		$\vdots$	$\vdots$		$\vdots$	

Tabla 4.1: *Número de polinomios para diferentes valores de p y n.*

representa un nivel de seguridad aceptable frente a este ataque. La tabla 4.1 muestra el número de polinomios totales a considerar para distintos valores de p y n.

Notemos que el protocolo 4.2 presenta cierta simetría en el sentido de que Alicia (y también Bernardo) utiliza el mismo polinomio para multiplicar por la izquierda y por la derecha el elemento $N \in R \setminus Z(R)$. Con el fin de evitar dicha simetría y con ello dificultar la labor de cualquier atacante, en el siguiente protocolo de intercambio la clave privada de cada uno de los usuarios está formada por dos polinomios con coeficientes en centro del anillo, como mostramos a continuación.

Protocolo 4.3: *Suponemos que los elementos $M \in R$ y $N \in R \setminus Z(R)$ son públicos.*

Paso 1: *Alicia elige su clave privada $f_1(\mathsf{X}), f_2(\mathsf{X}) \in Z(R)[\mathsf{X}]$ y $(r,s) \in \mathbb{N}^2$.*
Bernardo elige su clave privada $g_1(\mathsf{X}), g_2(\mathsf{X}) \in Z(R)[\mathsf{X}]$ y $(u,v) \in \mathbb{N}^2$.

Paso 2: *Alicia calcula su clave pública $P_A = f_1(M)^r N f_2(M)^s$ y se la envía a Bernardo.*

De forma similar, Bernardo calcula su clave privada $P_B = g_1(M)^u N g_2(M)^v$, *y se la envía a Alicia.*

Paso 3: *Alicia y Bernardo calculan* S_A *y* S_B, *respectivamente, como*

$$S_A = f_1(M)^r P_B f_2(M)^s \quad y \quad S_B = g_1(M)^u P_A g_2(M)^v.$$

Mediante un argumento análogo al del protocolo 4.2, tenemos que el secreto compartido es $S_A = S_B$, tal y como establece en el teorema que sigue.

Teorema 4.3: *Con la notación del protocolo 4.3, tenemos que* $S_A = S_B$.

DEMOSTRACIÓN: La demostración es consecuencia inmediata de la expresión (4.1).□

A continuación, desarrollamos, a modo de ejemplo, el funcionamiento del protocolo 4.3 sobre el anillo E_{31}.

Ejemplo 4.2: Para iniciar el protocolo 4.3 consideramos los mismos elementos públicos $M \in E_{31}$ y $N \in E_{31} \setminus Z(E_{31})$, utilizados en el ejemplo 4.1, con el fin de destacar las diferencias entre los dos protocolos.

Los pasos del protocolo son:

Paso 1: Alicia elige como su clave privada los enteros $(r, s) = (5, 7)$ y los polinomios $f_1(\mathsf{X})$, $f_2(\mathsf{X}) \in Z(E_{31})[\mathsf{X}]$, dados por las expresiones

$$f_1(\mathsf{X}) = \begin{bmatrix} 15 & 0 \\ 0 & 77 \end{bmatrix} + \begin{bmatrix} 2 & 0 \\ 0 & 777 \end{bmatrix} \mathsf{X}^2 + \begin{bmatrix} 17 & 0 \\ 0 & 482 \end{bmatrix} \mathsf{X}^4,$$

$$f_2(\mathsf{X}) = \begin{bmatrix} 7 & 0 \\ 0 & 472 \end{bmatrix} \mathsf{X} + \begin{bmatrix} 12 & 0 \\ 0 & 508 \end{bmatrix} \mathsf{X}^2 + \begin{bmatrix} 1 & 0 \\ 0 & 869 \end{bmatrix} \mathsf{X}^6.$$

Entonces calcula

$$f_1(M) = \begin{bmatrix} 4 & 13 \\ 124 & 295 \end{bmatrix} \quad \text{y} \quad f_2(M) = \begin{bmatrix} 3 & 7 \\ 806 & 50 \end{bmatrix}.$$

Bernardo elige como su clave privada $(u, v) = (9, 8)$ y los polinomios $g_1(\mathsf{X})$, $g_2(\mathsf{X}) \in Z\left(E_{31}\right)[\mathsf{X}]$, dados por las expresiones

$$g_1(\mathsf{X}) = \begin{bmatrix} 9 & 0 \\ 0 & 71 \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 713 \end{bmatrix} \mathsf{X} + \begin{bmatrix} 26 & 0 \\ 0 & 181 \end{bmatrix} \mathsf{X}^4 + \begin{bmatrix} 13 & 0 \\ 0 & 292 \end{bmatrix} \mathsf{X}^5,$$

$$g_2(\mathsf{X}) = \begin{bmatrix} 21 & 0 \\ 0 & 300 \end{bmatrix} + \begin{bmatrix} 4 & 0 \\ 0 & 531 \end{bmatrix} \mathsf{X}^2 + \begin{bmatrix} 30 & 0 \\ 0 & 61 \end{bmatrix} \mathsf{X}^3 + \begin{bmatrix} 14 & 0 \\ 0 & 262 \end{bmatrix} \mathsf{X}^4.$$

Entonces calcula

$$g_1(M) = \begin{bmatrix} 27 & 24 \\ 155 & 817 \end{bmatrix} \quad \text{y} \quad g_2(M) = \begin{bmatrix} 20 & 3 \\ 620 & 886 \end{bmatrix}.$$

Paso 2: Alicia calcula su clave pública P_A como

$$P_A = f_1(M)^r N f_2(M)^s = \begin{bmatrix} 2 & 3 \\ 341 & 826 \end{bmatrix}$$

y se la envía a Bernardo.

De forma análoga Bernardo calcula su clave pública P_B como

$$P_B = g_1(M)^u N g_2(M)^v = \begin{bmatrix} 4 & 1 \\ 217 & 522 \end{bmatrix},$$

y se la envía a Alicia.

Paso 3: Alicia calcula S_A como

$$S_A = f_1(M)^r P_B f_2(M)^s = \begin{bmatrix} 6 & 5 \\ 682 & 957 \end{bmatrix}.$$

Bob calcula S_B como

$$S_B = g_1(M)^u P_A g_2(M)^v = \begin{bmatrix} 6 & 5 \\ 682 & 957 \end{bmatrix}.$$

Como consecuencia del teorema 4.3, el secreto compartido es $S_A = S_B$.

Notemos que un atacante conoce M, puesto que es público, pero no conoce ninguno de los polinomios $f_1(\mathsf{X}), f_2(\mathsf{X}), g_1(\mathsf{X}), g_2(\mathsf{X}) \in Z(E_{31})[\mathsf{X}]$. Por tanto, no conoce los elementos

$$f_1(M)^r = \begin{bmatrix} 1 & 0 \\ 0 & 94 \end{bmatrix}, \quad f_2(M)^s = \begin{bmatrix} 17 & 15 \\ 217 & 162 \end{bmatrix},$$

$$g_1(M)^u = \begin{bmatrix} 23 & 0 \\ 0 & 178 \end{bmatrix}, \quad g_2(M)^v = \begin{bmatrix} 19 & 18 \\ 837 & 751 \end{bmatrix}.$$

Observemos que cualquier atacante que quiera descubrir el secreto compartido debe obtener los polinomios $f_1(\mathsf{X})$, $f_2(\mathsf{X})$, $g_1(\mathsf{X})$, y $g_2(\mathsf{X})$, para más tarde encontrar (r, s) y (u, v) a partir de las expresiones

$$f_1(M)^r N f_2(M)^s = P_A \quad \text{y} \quad g_1(M)^u N g_2(M)^v = P_B.$$

Esto es equivalente a resolver dos problemas de tipo DP. ■

Para este protocolo, como hemos visto, un usuario necesita dos polinomios de grados n_1 y n_2, respectivamente, para generar su clave privada; por tanto, el número de posibles polinomios con coeficientes en el centro de E_p es $(n_1+1)(n_2+1)p^4$ para cada usuario, lo que dificulta un ataque por fuerza bruta sobre el conjunto de los polinomios con coeficientes en el anillo.

A modo de ejemplo, si consideramos un primo p de alrededor de 60 cifras decimales y elegimos polinomios de grados $n_1 = 9$ y $n_2 = 10$ respectivamente, el número de polinomios que debe considerar un atacante es del orden de 10^{242}, lo que supone un incremento del nivel de seguridad frente a este ataque respecto del protocolo 4.2, sin aumentar las necesidades computacionales. La tabla 4.2 muestra el número de polinomios totales para distintos valores de los grados de los polinomios n_1, n_2, sobre el anillo E_{31}.

4.2.2 Análisis de la seguridad

En esta sección analizamos algunos posibles ataques sobre los protocolos propuestos. Notemos en primer lugar que cualquiera de los ataques clásicos sobre cuerpos finitos, como son el *Index-Calculus*,*Square Roots*, *Quadratic Sieve* o *Number Field*

E_{31}	Grado de los polinomios								
n_1 \ n_2	4	6	8	10	12	⋯	18	20	⋯
3	18470420	25858588	33246756	40634924	48023092	⋯	70187596	77575764	⋯
5	27705630	38787882	49870134	60952386	72034638	⋯	105281394	116363646	⋯
7	36940840	51717176	66493512	81269848	96046184	⋯	140375192	155151528	⋯
9	46176050	64646470	83116890	101587310	120057730	⋯	175468990	193939410	⋯
11	55411260	77575764	99740268	121904772	144069276	⋯	210562788	232727292	⋯
13	64646470	90505058	116363646	142222234	168080822	⋯	245656586	271515174	⋯
15	73881680	103434352	132987024	162539696	192092368	⋯	280750384	310303056	⋯
17	83116890	116363646	149610402	182857158	216103914	⋯	315844182	349090938	⋯
19	92352100	129292940	166233780	203174620	240115460	⋯	350937980	387878820	⋯
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	

Tabla 4.2: *Número de polinomios para diferentes valores de los grados n_2 y n_2 sobre E_{31}.*

Sieve, no son viables en estos protocolos ya que la estructura algebraica subyacente es un anillo finito no conmutativo. Además, tanto E_p como $Z(E_p)$ son anillos no euclidianos, por lo que cualquier ataque basado en el uso de la división euclidieana tampoco se puede aplicar a estos protocolos. Así, por ejemplo, el ataque propuesto por Dubois and Kammerer [23] para los protocolos diseñados por Boucher *et al.* [10] no es aplicable.

En la sección 4.2.1 mencionamos que la seguridad de estos protocolos se basa en la dificultad de resolver un problema DP, para el que no se conoce ningún algoritmo probabilístico que sea capaz de resolver el problema en tiempo polinómico sobre un anillo no conmutativo. En nuestro caso, para los protocolos 4.2 y 4.3, un atacante necesita resolver el problema DP a partir de la ecuaciones

$$X_A X_B = X_B X_A, \tag{4.2}$$

$$Y_A Y_B = Y_B Y_A, \tag{4.3}$$

$$X_A N Y_A = P_A, \tag{4.4}$$

$$X_B N Y_B = P_B, \tag{4.5}$$

donde P_A y P_B son las claves públicas de Alicia y Bernardo respectivamente. Los elementos $M \in R$, $N \in R \setminus Z(R)$ son también conocidos por cualquier atacante.

El primer objetivo de un atacante para romper el protocolo 4.2 consiste en encontar los elementos X_A, X_B, Y_A e Y_B. Para ello, el atacante debe encontrar dos

polinomios $h_1(\mathsf{X}), h_2(\mathsf{X}) \in Z(R)[\mathsf{X}]$ y $\alpha_1, \alpha_2, \beta_1, \beta_2 \in \mathbb{N}$ tales que

$$h_1(M)^{\alpha_1} = X_A, \quad h_1(M)^{\alpha_2} = Y_A \qquad \text{y} \qquad h_2(M)^{\beta_1} = X_B, \quad h_2(M)^{\beta_2} = Y_B,$$

en cuyo caso se satisfacen las condiciones (4.2) y (4.3). Por otra parte, los polinomios con coeficientes en el centro del anillo R representan un conjunto cuyo cardinal dependerá del número de elementos del centro del anillo sobre el que se definan los protocolos, como comentamos al tratar los ejemplos de los protocolos sobre los anillos E_p y ${E_p}^{(m)}$. Posteriormente, el atacante debe comprobar también que se satisfacen las condiciones (4.4) y (4.5). Esto conduce directamente a un ataque por fuerza bruta, que no es factible si el conjunto de polinomios con coeficientes en el centro es lo suficientemente grande.

Análogamente, para el protocolo 4.3, el atacante debe encontrar los elementos X_A, X_B, Y_A e Y_B, de la misma forma en en el caso anterior. Por tanto, es necesario encontrar polinomios $h_1(\mathsf{X}), k_1(\mathsf{X}), h_2(\mathsf{X}), k_2(\mathsf{X}) \in Z(R)[\mathsf{X}]$ y $\alpha_1, \alpha_2, \beta_1, \beta_2 \in \mathbb{N}$ tales que

$$h_1(M)^{\alpha_1} = X_A, \quad k_1(M)^{\alpha_2} = Y_A \qquad \text{y} \qquad h_2(M)^{\beta_1} = X_B, \quad k_2(M)^{\beta_2} = Y_B.$$

De esta forma se satisfacen las condiciones (4.2) y (4.3), pero el número de polinomios se ha incrementado considerablemente, lo cual representa una dificultad adicional en el caso de que el número de polinomios sea grande.

En el caso del anillo E_p, como comentamos en la sección 2.3.2, si p es un número suficientemente grande, la probabilidad de que un elemento elegido al azar de E_p sea invertible, es prácticamente del 100 % y, por tanto, un ataque basado en la existencia de elementos invertibles es viable. Basándose en esta idea, Kamal y Youssef [30] proponen un criptoanálisis de un protocolo similar a los protocolos 4.2 y 4.3, que también es válido para dichos protocolos y que comentamos seguidamente.

Recordemos que los elementos M, N, P_A y P_B son públicos en los protocolos 4.2 y 4.3. Supongamos que un atacante obtiene dos elementos $W_1, W_2 \in E_p$, tales que

$$W_1 M = M W_1, \tag{4.6}$$

$$W_2 M = M W_2, \tag{4.7}$$

$$P_B W_2 = W_1 N. \tag{4.8}$$

Entonces, como resultado de las condiciones (4.6) y (4.7) tenemos que

$$W_1 f(M)^h = f(M)^h W_1 \quad \text{y} \quad W_2 f(M)^h = f(M)^h W_2,$$

para cualquier $f(\mathsf{X}) \in Z(E_p)[\mathsf{X}]$ y cualquier $h \in \mathbb{N}$. Ahora, si W_2 es invertible entonces

$$\begin{aligned} W_1 P_A W_2^{-1} &= W_1 f(M)^r N f(M)^s W_2^{-1} \\ &= f(M)^r W_1 N W_2^{-1} f(M)^s \\ &= f(M)^r P_B f(M)^s \\ &= S_A, \end{aligned} \tag{4.9}$$

con lo cual el atacante obtiene el secreto compartido S_A.

La principal dificultad con la que se encuentra el atacante, es encontrar los elementos W_1 y W_2 de E_p que satisfacen las condiciones (4.6), (4.7) y (4.8) debido a que una vez obtenidos dichos elementos, la probabilidad de que sean invertibles en E_p es muy elevada como demostramos en el capítulo 2.

Podemos evitar este ataque si consideramos un anillo no conmutativo en el que prácticamente no haya elementos invertibles como ocurre con el anillo ${E_p}^{(m)}$ si elegimos el primo p y el entero $m \geq 2$ de forma adecuada tal y como demostramos en el capítulo 3.

A continuación mostramos a modo de ejemplo el funcionamiento del protocolo de intercambio de claves 4.2 sobre el anillo $E_3^{(5)}$. Hay que tener en cuenta que en las implementaciones prácticas reales debemos considerar un primo p y un entero $m \geq 2$ lo suficientemente elevados para evitar los ataques por fuerza bruta.

Ejemplo 4.3: Consideramos públicos los elementos $M \in E_3^{(5)}$ y $N \in E_3^{(5)} \setminus Z\left(E_3^{(5)}\right)$ dados por las expresiones

$$M = \begin{bmatrix} 1 & 0 & 2 & 0 & 2 \\ 6 & 1 & 6 & 2 & 1 \\ 9 & 0 & 5 & 26 & 10 \\ 27 & 18 & 6 & 51 & 3 \\ 0 & 0 & 18 & 3 & 56 \end{bmatrix} \quad \text{y} \quad N = \begin{bmatrix} 1 & 0 & 0 & 2 & 2 \\ 0 & 3 & 7 & 8 & 8 \\ 18 & 0 & 22 & 18 & 4 \\ 27 & 9 & 6 & 19 & 35 \\ 81 & 54 & 0 & 0 & 6 \end{bmatrix}.$$

Los pasos del protocolo son:

Paso 1: Alicia elige su clave privada formada por los enteros $(r, s) = (11, 6)$ y el polimomio $f(\mathsf{X}) \in Z\left(E_3^{(5)}\right)[\mathsf{X}]$, dado por la expresión

$$f(\mathsf{X}) = \begin{bmatrix} 0 & & & & \\ & 3 & & & \\ & & 12 & & \\ & & & 12 & \\ & & & & 12 \end{bmatrix} + \begin{bmatrix} 1 & & & & \\ & 4 & & & \\ & & 13 & & \\ & & & 40 & \\ & & & & 40 \end{bmatrix} \mathsf{X} + \begin{bmatrix} 1 & & & & \\ & 4 & & & \\ & & 13 & & \\ & & & 40 & \\ & & & & 121 \end{bmatrix} \mathsf{X}^3,$$

entonces calcula

$$f(M) = \begin{bmatrix} 2 & 0 & 1 & 0 & 2 \\ 6 & 2 & 6 & 4 & 8 \\ 18 & 0 & 22 & 1 & 7 \\ 27 & 63 & 66 & 15 & 66 \\ 81 & 162 & 225 & 60 & 169 \end{bmatrix}.$$

Bernardo elige su clave privada formada por los enteros $(u, v) = (12, 14)$ y el polinomio $g(\mathsf{X}) \in Z\left(E_3^{(5)}\right)[\mathsf{X}]$, definido como

$$g(\mathsf{X}) = \begin{bmatrix} 0 & & & & \\ & 0 & & & \\ & & 9 & & \\ & & & 9 & \\ & & & & 9 \end{bmatrix} + \begin{bmatrix} 1 & & & & \\ & 1 & & & \\ & & 10 & & \\ & & & 10 & \\ & & & & 91 \end{bmatrix} \mathsf{X} + \begin{bmatrix} 0 & & & & \\ & 3 & & & \\ & & 12 & & \\ & & & 12 & \\ & & & & 12 \end{bmatrix} \mathsf{X}^2$$

$$+ \begin{bmatrix} 0 & & & & \\ & 3 & & & \\ & & 12 & & \\ & & & 12 & \\ & & & & 93 \end{bmatrix} \mathsf{X}^3 + \begin{bmatrix} 1 & & & & \\ & 4 & & & \\ & & 4 & & \\ & & & 31 & \\ & & & & 31 \end{bmatrix} \mathsf{X}^4,$$

y calcula

$$g(M) = \begin{bmatrix} 2 & 0 & 2 & 1 & 0 \\ 3 & 2 & 6 & 1 & 4 \\ 9 & 9 & 21 & 3 & 24 \\ 27 & 63 & 36 & 9 & 36 \\ 81 & 216 & 27 & 45 & 210 \end{bmatrix}.$$

Paso 2: Alicia calcula su clave pública P_A como

$$P_A = f(M)^r N f(M)^s = \begin{bmatrix} 2 & 0 & 1 & 0 & 2 \\ 3 & 6 & 8 & 2 & 0 \\ 9 & 9 & 1 & 22 & 15 \\ 27 & 54 & 75 & 3 & 45 \\ 0 & 216 & 144 & 36 & 108 \end{bmatrix},$$

y se la envía a Bernardo.

De forma similar, Bernardo calcula su clave pública P_B como

$$P_B = g(M)^u N g(M)^v = \begin{bmatrix} 1 & 0 & 1 & 2 & 0 \\ 0 & 3 & 0 & 6 & 6 \\ 18 & 0 & 18 & 9 & 0 \\ 27 & 54 & 27 & 0 & 27 \\ 0 & 81 & 0 & 162 & 162 \end{bmatrix},$$

y se la envía a Alicia.

Paso 3: Alicia calcula S_A como

$$S_A = f(M)^r P_B f(M)^s = \begin{bmatrix} 2 & 0 & 2 & 1 & 0 \\ 3 & 6 & 3 & 0 & 3 \\ 9 & 0 & 9 & 18 & 0 \\ 27 & 27 & 27 & 27 & 54 \\ 81 & 162 & 81 & 0 & 81 \end{bmatrix}.$$

Bernardo calcula S_B como

$$S_B = g(M)^u P_A g(M)^v = \begin{bmatrix} 2 & 0 & 2 & 1 & 0 \\ 3 & 6 & 3 & 0 & 3 \\ 9 & 0 & 9 & 18 & 0 \\ 27 & 27 & 27 & 27 & 54 \\ 81 & 162 & 81 & 0 & 81 \end{bmatrix}.$$

Como consecuencia del teorema 4.2 el secreto compartido es $S_A = S_B$.

Notemos que un atacante, aunque puede conocer el elemento $M \in E_3^{(5)}$ al ser público, desconoce los polinomios los polinomios $f(\mathsf{X}), g(\mathsf{X}) \in Z\left(E_3^{(5)}\right)[\mathsf{X}]$ y los enteros (r, s) y (u, v), como ocurría con el ejemplo 4.1 definido sobre E_{31}. Como consecuencia de ello, son desconocidos los elementos

$$f(M)^r = \begin{bmatrix} 2 & 0 & 1 & 0 & 2 \\ 6 & 2 & 6 & 4 & 8 \\ 18 & 0 & 22 & 1 & 7 \\ 27 & 63 & 66 & 15 & 66 \\ 81 & 162 & 225 & 60 & 169 \end{bmatrix}^{11} = \begin{bmatrix} 2 & 0 & 1 & 0 & 1 \\ 3 & 5 & 3 & 1 & 8 \\ 18 & 0 & 1 & 25 & 26 \\ 54 & 9 & 66 & 21 & 24 \\ 0 & 81 & 36 & 33 & 22 \end{bmatrix},$$

$$f(M)^s = \begin{bmatrix} 2 & 0 & 1 & 0 & 2 \\ 6 & 2 & 6 & 4 & 8 \\ 18 & 0 & 22 & 1 & 7 \\ 27 & 63 & 66 & 15 & 66 \\ 81 & 162 & 225 & 60 & 169 \end{bmatrix}^{6} = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 3 & 5 & 0 \\ 0 & 9 & 25 & 1 & 6 \\ 54 & 45 & 57 & 21 & 18 \\ 162 & 216 & 225 & 96 & 118 \end{bmatrix},$$

$$g(M)^u = \begin{bmatrix} 2 & 0 & 2 & 1 & 0 \\ 3 & 2 & 6 & 1 & 4 \\ 9 & 9 & 21 & 3 & 24 \\ 27 & 63 & 36 & 9 & 36 \\ 81 & 216 & 27 & 45 & 210 \end{bmatrix}^{12} = \begin{bmatrix} 1 & 0 & 1 & 2 & 0 \\ 0 & 1 & 6 & 2 & 5 \\ 18 & 18 & 18 & 18 & 9 \\ 27 & 72 & 54 & 36 & 36 \\ 0 & 189 & 162 & 135 & 216 \end{bmatrix},$$

$$g(M)^v = \begin{bmatrix} 2 & 0 & 2 & 1 & 0 \\ 3 & 2 & 6 & 1 & 4 \\ 9 & 9 & 21 & 3 & 24 \\ 27 & 63 & 36 & 9 & 36 \\ 81 & 216 & 27 & 45 & 210 \end{bmatrix}^{14} = \begin{bmatrix} 1 & 0 & 1 & 2 & 0 \\ 3 & 4 & 0 & 5 & 2 \\ 18 & 18 & 18 & 18 & 9 \\ 0 & 45 & 27 & 9 & 63 \\ 81 & 27 & 0 & 216 & 135 \end{bmatrix}.$$

Supongamos que un atacante intercepta P_A y P_B. En primer lugar, para obtener el secreto compartido, el atacante debe determinar los polinomios $f(\mathsf{X})$ y $g(\mathsf{X})$, para obtener los pares (r, s) y (u, v) a partir de las expresiones

$$f(M)^r N f(M)^s = P_A \quad \text{y} \quad g(M)^u N g(M)^v = P_B.$$

Esto es equivalente, debido a que (r, s) y (u, v) son desconocidos, a resolver dos problemas de tipo DP. ■

Notemos, además, que los elementos $f(M)^r, f(M)^s, g(M)^u, g(M)^v, P_A$ y P_B no son invertibles en $E_3^{(5)}$ como consecuencia del teorema 3.3, lo que significa que tampoco es viable el ataque planteado por Kamal y Youssef [30].

Por otra parte, desarrollar un ataque por fuerza bruta sobre el conjunto de polinomios con coeficientes en el centro del anillo es inviable, debido a que el número de polinomios de grado n con coeficientes en el centro de ${E_p}^{(m)}$ es $(n+1)p^m$. Por tanto, para ${E_p}^{(m)}$ no sólo depende del primo p tomado sino también del entero $m \geq 2$ elegido. En consecuencia, si determinamos de forma adecuada el primo p, el entero $m \geq 2$ y el grado de los polinomios, es posible alcanzar un alto nivel de seguridad frente a este ataque.

Recordemos que sobre E_p consideramos seguro este intercambio respecto a este ataque si elegíamos un primo p de unas 60 cifras decimales y un polinomio de grado $n = 20$, lo que representaba un número de posibles polinomios del orden de 10^{121}. Sobre ${E_p}^{(m)}$ estas necesidades disminuyen considerablemente de forma que si tomamos p de unas 20 cifras decimales, $m = 5$ y polinomios de grado $n = 10$, conseguimos un nivel de seguridad similar ya que el número total de polinomios es del orden de 10^{121}.

La tabla 4.3 muestra el número de polinomios para distintos valores de los parámetros p, m y n. A modo de ejemplo, notemos que es suficiente tomar un primo p

$E_p^{(m)}$	m =5		m =10		m =20	
p \ n	3	5	3	5	3	5
2	128	192	4096	6144	4194304	6291456
3	972	1458	236196	354294	$1,40 \cdot 10^{10}$	$2,09 \cdot 10^{10}$
5	12500	18750	$3,91 \cdot 10^{7}$	$5,86 \cdot 10^{7}$	$3,82 \cdot 10^{14}$	$5,72 \cdot 10^{14}$
7	67228	100842	$1,13 \cdot 10^{9}$	$1,70 \cdot 10^{9}$	$3,19 \cdot 10^{17}$	$4,79 \cdot 10^{17}$
11	644204	966306	$1,04 \cdot 10^{11}$	$1,56 \cdot 10^{11}$	$2{,}69 \cdot 10^{21}$	$4,04 \cdot 10^{21}$
13	1485172	2227758	$5,51 \cdot 10^{11}$	$8,27 \cdot 10^{11}$	$7,60 \cdot 10^{22}$	$1,14 \cdot 10^{23}$
17	5679428	8519142	$8,06 \cdot 10^{12}$	$1,21 \cdot 10^{13}$	$1,63 \cdot 10^{25}$	$2,44 \cdot 10^{25}$
19	9904396	$1,24 \cdot 10^{7}$	$2,45 \cdot 10^{13}$	$3,68 \cdot 10^{13}$	$1,50 \cdot 10^{26}$	$2,26 \cdot 10^{26}$
23	$2,58 \cdot 10^{7}$	$3,86 \cdot 10^{7}$	$1,66 \cdot 10^{14}$	$2,49 \cdot 10^{14}$	$6,87 \cdot 10^{27}$	$1,03 \cdot 10^{28}$
29	$8,21 \cdot 10^{7}$	$1,23 \cdot 10^{8}$	$1,68 \cdot 10^{15}$	$2,52 \cdot 10^{15}$	$7,08 \cdot 10^{29}$	$1,06 \cdot 10^{30}$
31	$1,15 \cdot 10^{8}$	$1,72 \cdot 10^{8}$	$3,28 \cdot 10^{15}$	$4,92 \cdot 10^{15}$	$2,69 \cdot 10^{30}$	$4,03 \cdot 10^{30}$
⋮	⋮	⋮	⋮	⋮	⋮	⋮
97	$3,44 \cdot 10^{10}$	$5,15 \cdot 10^{10}$	$2,95 \cdot 10^{20}$	$4,43 \cdot 10^{20}$	$2,18 \cdot 10^{40}$	$3,26 \cdot 10^{40}$
101	$4{,}20 \cdot 10^{10}$	$6,31 \cdot 10^{10}$	$4,42 \cdot 10^{20}$	$6,63 \cdot 10^{20}$	$4,88 \cdot 10^{40}$	$7,32 \cdot 10^{40}$
103	$4,64 \cdot 10^{10}$	$6,96 \cdot 10^{10}$	$5,38 \cdot 10^{20}$	$8,06 \cdot 10^{20}$	$7,23 \cdot 10^{40}$	$1,08 \cdot 10^{41}$
107	$5,61 \cdot 10^{10}$	$8,42 \cdot 10^{10}$	$7,88 \cdot 10^{20}$	$1,18 \cdot 10^{21}$	$1,55 \cdot 10^{41}$	$2,32 \cdot 10^{41}$
109	$6,16 \cdot 10^{10}$	$9,23 \cdot 10^{10}$	$9,47 \cdot 10^{20}$	$1,42 \cdot 10^{21}$	$2,24 \cdot 10^{41}$	$3{,}26 \cdot 10^{41}$
⋮	⋮	⋮	⋮	⋮	⋮	⋮
199	$1,25 \cdot 10^{12}$	$1,87 \cdot 10^{12}$	$3,90 \cdot 10^{23}$	$5,84 \cdot 10^{23}$	$3,79 \cdot 10^{46}$	$5,69 \cdot 10^{46}$
211	$1,67 \cdot 10^{12}$	$2,51 \cdot 10^{12}$	$7,00 \cdot 10^{23}$	$1,05 \cdot 10^{24}$	$1,22 \cdot 10^{47}$	$1,84 \cdot 10^{47}$
223	$2,21 \cdot 10^{12}$	$3,31 \cdot 10^{12}$	$1,22 \cdot 10^{24}$	$1,83 \cdot 10^{24}$	$3,70 \cdot 10^{47}$	$5,55 \cdot 10^{47}$
⋮	⋮	⋮	⋮	⋮	⋮	⋮
997	$3,94 \cdot 10^{15}$	$5,91 \cdot 10^{15}$	$3,88 \cdot 10^{30}$	$5,82 \cdot 10^{30}$	$3,77 \cdot 10^{60}$	$5,65 \cdot 10^{60}$
1009	$4,18 \cdot 10^{15}$	$6,28 \cdot 10^{15}$	$4,38 \cdot 10^{30}$	$6,56 \cdot 10^{30}$	$4,79 \cdot 10^{60}$	$7,18 \cdot 10^{60}$
⋮	⋮	⋮	⋮	⋮	⋮	⋮
10007	$4,01 \cdot 10^{20}$	$6,02 \cdot 10^{20}$	$4,03 \cdot 10^{40}$	$6,04 \cdot 10^{40}$	$4,06 \cdot 10^{80}$	$6,09 \cdot 10^{80}$
⋮	⋮	⋮	⋮	⋮	⋮	⋮
1150249	$8,05 \cdot 10^{30}$	$1,21 \cdot 10^{31}$	$1,62 \cdot 10^{61}$	$2,43 \cdot 10^{61}$	$6,58 \cdot 10^{121}$	$9,86 \cdot 10^{121}$
⋮	⋮	⋮	⋮	⋮	⋮	⋮

Tabla 4.3: *Número de polinomios en* $Z\left(E_p{}^{(m)}\right)$.

de 7 cifras como es $p = 1150249$, $m = 20$ y polinomios de grado $n = 5$ para alcanzar del orden de 10^{121} posibles polinomios y mantener, por tanto, el nivel de seguridad.

No desarrollamos con detalle un ejemplo para el protocolo 4.3 sobre el anillo $E_3^{(5)}$ debido a su gran similitud con el ejemplo mostrado anteriormente para el protoco-

$E_3^{(5)}$	Grado de los polinomios								
n_1 \ n_2	4	6	8	10	12	⋯	18	20	⋯
3	1180980	1653372	2125764	2598156	3070548	⋯	4487724	4960116	⋯
5	1771470	2480058	3188646	3897234	4605822	⋯	6731586	7440174	⋯
7	2361960	3306744	4251528	5196312	6141096	⋯	8975448	9920232	⋯
9	2952450	4133430	5314410	6495390	7676370	⋯	11219310	12400290	⋯
11	3542940	4960116	6377292	7794468	9211644	⋯	13463172	14880348	⋯
13	4133430	5786802	7440174	9093546	10746918	⋯	15707034	17360406	⋯
15	4723920	6613488	8503056	10392624	12282192	⋯	17950896	19840464	⋯
17	5314410	7440174	9565938	11691702	13817466	⋯	20194758	22320522	⋯
19	5904900	8266860	10628820	12990780	15352740	⋯	22438620	24800580	⋯
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	

Tabla 4.4: *Número de polinomios con coeficientes en el centro de* $E_3^{(5)}$

lo 4.2. Sin embargo, destacamos sus diferencias de una manera concisa.

Si seguimos los pasos del protocolo 4.3, Alicia elige como clave privada los enteros positivos (r, s) y los polinomios $f_1(\mathsf{X})$ y $f_2(\mathsf{X})$ con coeficientes en el centro del anillo. Bernardo por su parte elige como su clave privada los enteros (u, v) y los polinomios con coeficientes en el centro del anillo $g_1(\mathsf{X})$ y $g_2(\mathsf{X})$.

De esta forma, cualquier atacante que pretenda descubrir el secreto compartido debe obtener los polinomios $f_1(\mathsf{X})$, $f_2(\mathsf{X})$, $g_1(\mathsf{X})$, y $g_2(\mathsf{X})$, con el fin de encontrar los enteros (r, s) y (u, v) que verifiquen las expresiones

$$f_1(M)^r N f_2(M)^s = P_A \quad \text{y} \quad g_1(M)^u N g_2(M)^v = P_B.$$

Esto es equivalente a resolver dos problemas de tipo DP.

En este caso, un ataque por fuerza bruta sobre el conjunto de polinomios con coeficientes en el centro del anillo es incluso menos viable que en el protocolo 4.2, debido a que cada usuario elige dos polinomios para su clave privada. En consecuencia, el cardinal de polinomios con coeficientes en el centro de ${E_p}^{(m)}$ es $(n_1+1)(n_2+1)p^2m$, con n_1 y n_2 el grado de cada uno de los dos polinomios elegidos para la clave secreta de cada usuario.

Las tablas 4.4, 4.5 y 4.6 muestran el cardinal del conjunto de polinomios con coeficientes en el centro de $E_3^{(5)}$, $E_3^{(10)}$ y $E_3^{(20)}$, respectivamente, a modo de ejemplo.

Recordemos que sobre E_p, el protocolo 4.3 es seguro frente al ataque por fuerza

$E_3^{(10)}$	Grado de los polinomios								
n_1 \ n_2	4	6	8	10	12	$\cdots$	18	20	$\cdots$
3	$6,97 \cdot 10^{10}$	$9,76 \cdot 10^{10}$	$1,26 \cdot 10^{11}$	$1,53 \cdot 10^{11}$	$1,81 \cdot 10^{11}$	$\cdots$	$2,65 \cdot 10^{11}$	$2,93 \cdot 10^{11}$	$\cdots$
5	$1,05 \cdot 10^{11}$	$1,47 \cdot 10^{11}$	$1,88 \cdot 10^{11}$	$2,30 \cdot 10^{11}$	$2,72 \cdot 10^{11}$	$\cdots$	$3,92 \cdot 10^{11}$	$4,39 \cdot 10^{11}$	$\cdots$
7	$1,40 \cdot 10^{11}$	$1,95 \cdot 10^{11}$	$2,51 \cdot 10^{11}$	$3,07 \cdot 10^{11}$	$3,63 \cdot 10^{11}$	$\cdots$	$5,30 \cdot 10^{11}$	$5,86 \cdot 10^{11}$	$\cdots$
9	$1,74 \cdot 10^{11}$	$2,44 \cdot 10^{11}$	$3,14 \cdot 10^{11}$	$3,84 \cdot 10^{11}$	$4,53 \cdot 10^{11}$	$\cdots$	$6,63 \cdot 10^{11}$	$7,32 \cdot 10^{11}$	$\cdots$
11	$2,09 \cdot 10^{11}$	$2,93 \cdot 10^{11}$	$3,77 \cdot 10^{11}$	$4,60 \cdot 10^{11}$	$5,44 \cdot 10^{11}$	$\cdots$	$7,95 \cdot 10^{11}$	$8,79 \cdot 10^{11}$	$\cdots$
13	$2,44 \cdot 10^{11}$	$3,42 \cdot 10^{11}$	$4,40 \cdot 10^{11}$	$5,37 \cdot 10^{11}$	$6,35 \cdot 10^{11}$	$\cdots$	$9,28 \cdot 10^{11}$	$1,03 \cdot 10^{12}$	$\cdots$
15	$2,79 \cdot 10^{11}$	$3,91 \cdot 10^{11}$	$5,02 \cdot 10^{11}$	$6,14 \cdot 10^{11}$	$7,25 \cdot 10^{11}$	$\cdots$	$1,06 \cdot 10^{12}$	$1,17 \cdot 10^{12}$	$\cdots$
17	$3,14 \cdot 10^{11}$	$4,39 \cdot 10^{11}$	$5,65 \cdot 10^{11}$	$6,90 \cdot 10^{11}$	$8,16 \cdot 10^{11}$	$\cdots$	$1,19 \cdot 10^{12}$	$1,32 \cdot 10^{12}$	$\cdots$
19	$3,49 \cdot 10^{11}$	$4,88 \cdot 10^{11}$	$6,28 \cdot 10^{11}$	$7,67 \cdot 10^{11}$	$9,06 \cdot 10^{11}$	$\cdots$	$1,33 \cdot 10^{12}$	$1,47 \cdot 10^{12}$	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	

Tabla 4.5: *Número de polinomios con coeficientes en el centro de* $E_3^{(10)}$

$E_3^{(20)}$	Grado de los polinomios								
n_1 \ n_2	4	6	8	10	12	$\cdots$	18	20	$\cdots$
3	$2,43 \cdot 10^{20}$	$3,40 \cdot 10^{20}$	$4,38 \cdot 10^{20}$	$5,35 \cdot 10^{20}$	$6,32 \cdot 10^{20}$	$\cdots$	$9,24 \cdot 10^{20}$	$1,02 \cdot 10^{21}$	$\cdots$
5	$3,65 \cdot 10^{20}$	$5,11 \cdot 10^{20}$	$6,57 \cdot 10^{20}$	$8,02 \cdot 10^{20}$	$9,48 \cdot 10^{20}$	$\cdots$	$1,39 \cdot 10^{21}$	$1,53 \cdot 10^{21}$	$\cdots$
7	$4,86 \cdot 10^{20}$	$6,81 \cdot 10^{20}$	$8,75 \cdot 10^{20}$	$1,07 \cdot 10^{21}$	$1,26 \cdot 10^{21}$	$\cdots$	$1,85 \cdot 10^{21}$	$2,04 \cdot 10^{21}$	$\cdots$
9	$6,08 \cdot 10^{20}$	$8,51 \cdot 10^{20}$	$1,09 \cdot 10^{21}$	$1,34 \cdot 10^{21}$	$1,58 \cdot 10^{21}$	$\cdots$	$2,31 \cdot 10^{21}$	$2,55 \cdot 10^{21}$	$\cdots$
11	$7,30 \cdot 10^{20}$	$1,02 \cdot 10^{21}$	$1,31 \cdot 10^{21}$	$1,61 \cdot 10^{21}$	$1,90 \cdot 10^{21}$	$\cdots$	$2,77 \cdot 10^{21}$	$3,06 \cdot 10^{21}$	$\cdots$
13	$8,51 \cdot 10^{20}$	$1,19 \cdot 10^{21}$	$1,53 \cdot 10^{21}$	$1,87 \cdot 10^{21}$	$2,21 \cdot 10^{21}$	$\cdots$	$3,23 \cdot 10^{21}$	$3,57 \cdot 10^{21}$	$\cdots$
15	$9,73 \cdot 10^{20}$	$1,36 \cdot 10^{21}$	$1,75 \cdot 10^{21}$	$2,14 \cdot 10^{21}$	$2,53 \cdot 10^{21}$	$\cdots$	$3,70 \cdot 10^{21}$	$4,09 \cdot 10^{21}$	$\cdots$
17	$1,09 \cdot 10^{21}$	$1,53 \cdot 10^{21}$	$1,97 \cdot 10^{21}$	$2,41 \cdot 10^{21}$	$2,85 \cdot 10^{21}$	$\cdots$	$4,16 \cdot 10^{21}$	$4,60 \cdot 10^{21}$	$\cdots$
19	$1,22 \cdot 10^{21}$	$1,70 \cdot 10^{21}$	$2,19 \cdot 10^{21}$	$2,68 \cdot 10^{21}$	$3,16 \cdot 10^{21}$	$\cdots$	$4,62 \cdot 10^{21}$	$5,11 \cdot 10^{21}$	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	

Tabla 4.6: *Número de polinomios con coeficientes en el centro de* $E_3^{(20)}$

bruta sobre el cardinal del conjunto de los polinomios, si tomamos un número primo p de alrededor de 60 cifras y elegimos polinomios de grados $n_1 = 9$ y $n_2 = 10$, para los cuales se obtienen del orden de 10^{242} polinomios. Sobre ${E_p}^{(m)}$ estas necesidades disminuyen de forma considerable, ya que si tomamos $m = 10$ y polinomios de grados $n_1 = 9$ y $n_2 = 10$, para alcanzar un cardinal de polinomios con coeficientes en el centro de ${E_p}^{(m)}$ del orden de 10^{242}, es suficiente elegir un primo p de unas 12 cifras decimales. Si consideramos $m = 20$, $n_1 = 9$ y $n_2 = 10$, es suficiente elegir un primo p de 6 cifras decimales para obtener del orden de 10^{242} polinomios con

coeficientes en el centro de ${E_p}^{(m)}$. Por ejemplo, si $p = 1150249$, $n_1 = 9$ y $n_2 = 10$, para $m = 20$, tenemos del orden de $2,47 \cdot 10^{244}$ polinomios.

4.3 Multidifusión de claves

Los modelos de comunicación que proponemos en esta sección son esquemas de tipo *Multicast* sobre anillos no conmutativos en el marco de los modelos *IP-Multicast*. Notemos que desarrollamos las comunicaciones en un grupo restringido de *usuarios* que manejan todas las operaciones de cambio, intercambio y difusión de claves por sí mismos.

Steiner, Tsudik y Waidner [54] introdujeron dos nuevos esquemas de intercambio múltiple como extensión del modelo de intercambio de claves de Diffie-Hellman. Uno de estos protocolos, conocido por el nombre de *CLIQUES*, es utilizado como base por algunos autores [55] para protocolos de intercambio de claves en grupo dinámicos (*Dynamic Peer Groups*).

Esta sección está dedicada al estudio de dos esquemas de multidifusión de claves de tipo distribuido, definidos sobre un anillo no conmutativo cualquiera R, donde aseguremos que el número de elementos invertibles es bajo en relación al cardinal total del anillo. A continuación, se desarrollan estos esquemas con algunos ejemplos sobre los anillos E_p y ${E_p}^{(m)}$ introducidos en los capítulos 2 y 3, respectivamente.

Antes de comenzar a introducir los protocolos consideramos que el conjunto de usuarios que pretenden intercambiar entre ellos información de forma segura sobre un canal inseguro es $\{U_1, U_2, \ldots, U_h\}$. Para ello debemos suponer que inicialmente los usuarios se han puesto de acuerdo en utilizar el mismo anillo no conmutativo R como base del proceso de intercambio.

Recordemos, como vimos en la sección 4.2.1, que en un anillo no conmutativo cualquiera R, si $f(\mathsf{x}), g(\mathsf{x}) \in Z(R)[\mathsf{x}]$ y $M \in R$, para cualesquiera que sean los enteros positivos r y s, se cumple

$$f(M)^r g(M)^s = g(M)^r f(M)^s. \tag{4.10}$$

4.3.1 Esquema de multidifusión secuencial

Protocolo 4.4: *Cada uno de los usuarios U_i, para $i = 1, 2, \ldots, h$ elige un polinomio $f_i(\mathsf{X}) \in Z(R)[\mathsf{X}]$ y un par de enteros positivos r_i and s_i. De esta forma la clave privada de cada usuario U_i está formada por la terna $(f_i(\mathsf{X}), r_i, s_i)$.*

Consideramos el elemento público $K_0 = N \in R \setminus Z(R)$.

El esquema sigue los siguientes pasos:

(a) *El usuario U_1 calcula el elemento K_1 de R como*

$$K_1 = f_1(M)^{r_1} K_0 f_1(M)^{s_1}. \tag{4.11}$$

A continuación el usuario U_1 envía el elemento K_1 al usuario U_2.

(b) *El usuario U_2 calcula el elemento $K_2 \in R$ como*

$$K_2 = f_2(M)^{r_2} K_1 f_2(M)^{s_2}, \tag{4.12}$$

de forma que el usuario U_2 envía al usuario U_3 el vector (K_1, K_2) de elementos de R.

(c) *Generalizando el proceso, para $i = 3, 4, \ldots, h-2, h-1$, el usuario U_i calcula el elemento*

$$K_i = f_i(M)^{r_i} K_{i-1} f_i(M)^{s_i} \in R. \tag{4.13}$$

Entonces, el usuario U_i envía al usuario U_{i+1} el vector $(K_1, K_2, \ldots, K_{i-1}, K_i)$ de elementos de R.

(d) *Cuando el usuario U_h recibe el vector $(K_1, K_2, \ldots, K_{h-2}, K_{h-1})$, calcula el elemento*

$$L_l^{(h)} = f_h(M)^{r_h} K_l f_h(M)^{s_h} \in R, \tag{4.14}$$

con $l = 0, 1, 2, \ldots, h-2, h-1$.

Entonces el usuario U_h envía al usuario U_{h-1} el vector $\left(L_0^{(h)}, L_1^{(h)}, \ldots, L_{h-3}^{(h)}, L_{h-2}^{(h)}\right)$ de elementos de R.

(e) *Cuando el usuario U_{h-1} recibe el vector $\left(L_0^{(h)}, L_1^{(h)}, \ldots, L_{h-3}^{(h)}, L_{h-2}^{(h)}\right)$ del usuario U_h, entonces calcula el elemento*

$$L_l^{(h-1)} = f_{h-1}(M)^{r_{h-1}} L_l^{(h)} f_{h-1}(M)^{s_{h-1}} \in R, \tag{4.15}$$

con $l = 0, 1, 2, \ldots, h-3, h-2$.

El usuario U_{h-1} *envía al usuario* U_{h-2} *el vector* $\left(L_0^{(h-1)}, L_1^{(h-1)}, \ldots, L_{h-4}^{(h-1)}, L_{h-3}^{(h-1)}\right)$ *de elementos de* R.

(f) *Este proceso se generaliza para* $i = 2, 3, \ldots, h-2, h-1$, *de forma que cuando el usuario* U_{h-i} *recibe del usuario* U_{h-i+1} *el vector de elementos de* R *dado por*

$$\left(L_0^{(h-i+1)}, L_1^{(h-i+1)}, \ldots, L_{h-i-2}^{(h-i+1)}, L_{h-i-1}^{(h-i+1)}\right),$$

calcula el elemento

$$L_l^{(h-i)} = f_{h-i}(M)^{r_{h-i}} L_l^{(h-i+1)} f_{h-i}(M)^{s_{h-i}}, \tag{4.16}$$

con $l = 0, 1, 2, \ldots, h-i-2, h-i-1$.

Seguidamente el usuario U_{h-i} *envía el vector* $\left(L_0^{(h-i)}, L_1^{(h-i)}, \ldots, L_{h-i-3}^{(h-i)}, L_{h-i-2}^{(h-i)}\right)$ *de elementos de* R *al usuario* U_{h-i-1}.

(g) *Por último cada uno de los usuarios* U_{h-i}, *para* $i = 0, 1, 2, \ldots, h-2, h-1$, *ha calculado el elemento* $S_{h-i} = L_{h-i-1}^{(h-i)} \in R$. *Notemos que éste es el único elemento que no ha sido enviado al usuario* U_{h-i-1}.

Es fácil observar que el secreto compartido por todos los usuarios del sistema es $S_{h-i} = L_{h-i-1}^{(h-i)}$, como demostramos a continuación.

Teorema 4.4: *Con la notación del esquema 4.4, todos los usuarios comparten el mismo secreto. En particular, para* $i = 0, 1, 2, \ldots, h-2, h-1$, *tenemos que*

$$L_{h-i-1}^{(h-i)} = \left(\prod_{k=1}^{h} f_k(M)^{r_k}\right) K_0 \left(\prod_{k=1}^{h} f_k(M)^{s_k}\right) = S_{h-i}.$$

DEMOSTRACIÓN: Supongamos que $i \in \{0, 1, 2, \ldots, h-2, h-1\}$. Como consecuencia de las expresiones (4.16), (4.15), (4.14) y (4.10) tenemos que

$$\begin{aligned} L_{h-i-1}^{(h-i)} &= f_{h-i}(M)^{r_{h-i}} L_{h-i-1}^{(h-i+1)} f_{h-i}(M)^{s_{h-i}} \\ &= f_{h-i}(M)^{r_{h-i}} \left(f_{h-i+1}(M)^{r_{h-i+1}} L_{h-i-1}^{(h-i+2)} f_{h-i+1}(M)^{s_{h-i+1}}\right) f_{h-i}(M)^{s_{h-i}} \end{aligned}$$

$$= \cdots$$

$$= \left(\prod_{k=h-i}^{h} f_k(M)^{r_k}\right) K_{h-i-1} \left(\prod_{k=h-i}^{h} f_k(M)^{s_k}\right) \in R \tag{4.17}$$

Por otro lado, de las expresiones (4.11), (4.12), (4.13), y (4.10) tenemos que

$$\begin{aligned} K_{h-i-1} &= f_{h-i-1}(M)^{r_{h-i-1}} K_{h-i-2} f_{h-i-1}(M)^{s_{h-i-1}} \\ &= f_{h-i-1}(M)^{r_{h-i-1}} \left(f_{h-i-2}(M)^{r_{h-i-2}} K_{h-i-3} f_{h-i-2}(M)^{s_{h-i-2}}\right) f_{h-i-1}(M)^{s_{h-i-1}} \\ &= \cdots \\ &= \left(\prod_{k=1}^{h-i-1} f_k(M)^{r_k}\right) K_0 \left(\prod_{k=1}^{h-i-1} f_k(M)^{s_k}\right) \in R \end{aligned} \tag{4.18}$$

Por último, como consecuencia de las expresiones (4.17), (4.18) y (4.10) tenemos que

$$\begin{aligned} L_{h-i-1}^{(h-i)} &= \left(\prod_{k=h-i}^{h} f_k(M)^{r_k}\right) \left(\prod_{k=1}^{h-i-1} f_k(M)^{r_k}\right) K_0 \left(\prod_{k=1}^{h-i-1} f_k(M)^{s_k}\right) \left(\prod_{k=h-i}^{h} f_k(M)^{s_k}\right) \\ &= \left(\prod_{k=1}^{h} f_k(M)^{r_k}\right) K_0 \left(\prod_{k=1}^{h} f_k(M)^{s_k}\right) = S_{h-i} \in R. \end{aligned}$$ □

Cuando un nuevo usuario U_{h+1} quiere unirse al sistema (operación *join*) es necesesario preservar el secreto compartido. Para ello, el usuario U_h debe cambiar su clave secreta, lo que significa que debe elegir un nuevo polinomio $\widehat{f_h} \in Z(R)[\mathsf{X}]$ y dos nuevos números naturales $\widehat{r}_h$ y $\widehat{s}_h$. Entonces, el usuario U_h calcula el elemento

$$\begin{aligned} \widehat{K}_h &= \widehat{f_h}(M)^{\widehat{r}_h} K_{h-1} \widehat{f_h}(M)^{\widehat{s}_h} \\ &= \left(\widehat{f_h}(M)^{\widehat{r}_h} \prod_{k=1}^{h-1} f_k(M)^{s_k}\right) K_0 \left(\widehat{f_h}(M)^{\widehat{r}_h} \prod_{k=1}^{h-1} f_k(M)^{s_k}\right). \end{aligned}$$

El usuario U_h envía al usuario U_{h+1} el vector $(K_1, K_2, \ldots, K_{h-1}, \widehat{K}_h)$ de elementos de R.

Entonces, el usuario U_{h+1} elige como su clave secreta $(f_{h+1}(\mathsf{X}), r_{h+1}, s_{h+1})$ y calcula

$$L_i^{(h+1)} = f_{h+1}(M)^{r_{h+1}} K_i f_{h+1}(M)^{s_{h+1}} \in R, \quad \text{para} \quad i = 0, 1, 2, \ldots, h-2, h-1.$$

$$L_h^{(h+1)} = f_{h+1}(M)^{r_{h+1}} \widehat{K}_h f_{h+1}(M)^{s_{h+1}} \in {E_p}^{(m)},$$

de esta forma le envía al usuario U_h el vector $\left(L_0^{(h+1)}, L_1^{(h+1)}, \ldots, L_{h-2}^{(h+1)}, L_{h-1}^{(h+1)}\right)$. Esta operación corresponde al paso (d) del esquema 4.4 para el usuario U_{h+1} en lugar del usuario U_h.

A continuación, los demás usuarios siguen el proceso descrito en los pasos (e) y (f) del esquema 4.4, empezando por el usuario U_h en lugar del usuario U_{h-1}.

Si cualquier usuario U_i decide abandonar el sistema, (operación *leave*) se requiere también un cambio de clave para preservar el secreto compartido.

En este caso, el proceso es bastante sencillo porque es suficiente que el usuario U_{i-1} mantenga guardada la información recibida por el usuario U_{i-2}. De esta forma el usuario U_{i-1} cambia su clave privada, para ello elige dos nuevos naturales cualesquiera y un nuevo polinomio con coeficientes en el centro de R, tal y como se hizo en la operación de unión al sistema, empezando el proceso de intercambio con el usuario U_{i-1}.

Observemos que en el caso particular de que el último usuario, U_h, abandone (*leave*) el sistema, entonces el usuario U_{h-1} cambia su clave privada (tal como ya hemos comentado) y devuelve la información a los demás usuarios del sistema, convirtiéndose el usuario U_{h-1} en el último usuario del nuevo sistema.

A continuación, mostramos mediante un ejemplo el funcionamiento del esquema definido anteriormente, para un sistema formado por cuatro usuarios. En el ejemplo consideramos el anillo $E_2^{(5)}$. Utilizamos valores pequeños de los parámetros para que puedan seguirse fácilmente las operaciones. En un caso práctico real, necesitaríamos aumentar el valor de estos parámetros para evitar un ataque por fuerza bruta.

Ejemplo 4.4: Consideramos los elementos

$$M = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 2 & 3 & 2 & 7 \\ 8 & 0 & 2 & 14 & 0 \\ 0 & 8 & 4 & 2 & 23 \end{bmatrix} \in E_2^{(5)} \quad \text{y} \quad N = \begin{bmatrix} 1 & 1 & 0 & 1 & 1 \\ 2 & 0 & 0 & 2 & 3 \\ 4 & 0 & 5 & 1 & 2 \\ 0 & 0 & 0 & 7 & 15 \\ 0 & 8 & 0 & 0 & 5 \end{bmatrix} \in E_2^{(5)} \setminus Z\left(E_2^{(5)}\right),$$

que son públicos.

Cada usuario U_i, con $i = 1, 2, 3, 4$, elige su clave privada, que viene dada por la terna $(r_i, s_i, f_i(\mathsf{X}))$, con los enteros positivos

$$(r_1, r_2, r_3, r_4) = (10, 5, 6, 11), \quad (s_1, s_2, s_3, s_4) = (5, 14, 16, 12),$$

y los polinomios $f_i(\mathsf{X}) \in Z\left(E_2^{(5)}\right)$ con $i = 1, 2, 3, 4$, dados por las expresiones

$$f_1(\mathsf{X}) = \begin{bmatrix} 1 & & & & \\ & 3 & & & \\ & & 3 & & \\ & & & 11 & \\ & & & & 11 \end{bmatrix} + \begin{bmatrix} 0 & & & & \\ & 2 & & & \\ & & 2 & & \\ & & & 10 & \\ & & & & 26 \end{bmatrix} \mathsf{X}^2 + \begin{bmatrix} 1 & & & & \\ & 1 & & & \\ & & 1 & & \\ & & & 1 & \\ & & & & 17 \end{bmatrix} \mathsf{X}^3$$
$$+ \begin{bmatrix} 1 & & & & \\ & 1 & & & \\ & & 5 & & \\ & & & 13 & \\ & & & & 29 \end{bmatrix} \mathsf{X}^4,$$

$$f_2(\mathsf{X}) = \begin{bmatrix} 1 & & & & \\ & 1 & & & \\ & & 1 & & \\ & & & 9 & \\ & & & & 25 \end{bmatrix} + \begin{bmatrix} 0 & & & & \\ & 2 & & & \\ & & 2 & & \\ & & & 10 & \\ & & & & 26 \end{bmatrix} \mathsf{X}^2 + \begin{bmatrix} 1 & & & & \\ & 3 & & & \\ & & 7 & & \\ & & & 7 & \\ & & & & 23 \end{bmatrix} \mathsf{X}^3$$
$$+ \begin{bmatrix} 0 & & & & \\ & 2 & & & \\ & & 6 & & \\ & & & 6 & \\ & & & & 6 \end{bmatrix} \mathsf{X}^4 + \begin{bmatrix} 0 & & & & \\ & 2 & & & \\ & & 6 & & \\ & & & 6 & \\ & & & & 22 \end{bmatrix} \mathsf{X}^5 + \begin{bmatrix} 1 & & & & \\ & 1 & & & \\ & & 5 & & \\ & & & 5 & \\ & & & & 21 \end{bmatrix} \mathsf{X}^6,$$

$$f_3(\mathsf{X}) = \begin{bmatrix} 0 & & & & \\ & 0 & & & \\ & & 0 & & \\ & & & 0 & \\ & & & & 16 \end{bmatrix} + \begin{bmatrix} 0 & & & & \\ & 2 & & & \\ & & 2 & & \\ & & & 2 & \\ & & & & 2 \end{bmatrix} \mathsf{X} + \begin{bmatrix} 1 & & & & \\ & 1 & & & \\ & & 1 & & \\ & & & 1 & \\ & & & & 17 \end{bmatrix} \mathsf{X}^2,$$

$$f_4(\mathsf{X}) = \begin{bmatrix} 0 & & & & \\ & 2 & & & \\ & & 2 & & \\ & & & 10 & \\ & & & & 10 \end{bmatrix} + \begin{bmatrix} 1 & & & & \\ & 1 & & & \\ & & 1 & & \\ & & & 1 & \\ & & & & 17 \end{bmatrix} \mathsf{X} + \begin{bmatrix} 1 & & & & \\ & 3 & & & \\ & & 3 & & \\ & & & 11 & \\ & & & & 27 \end{bmatrix} \mathsf{X}^2$$
$$+ \begin{bmatrix} 1 & & & & \\ & 3 & & & \\ & & 7 & & \\ & & & 7 & \\ & & & & 23 \end{bmatrix} \mathsf{X}^3 + \begin{bmatrix} 0 & & & & \\ & 0 & & & \\ & & 4 & & \\ & & & 4 & \\ & & & & 4 \end{bmatrix} \mathsf{X}^4 + \begin{bmatrix} 1 & & & & \\ & 3 & & & \\ & & 3 & & \\ & & & 11 & \\ & & & & 11 \end{bmatrix} \mathsf{X}^5$$
$$+ \begin{bmatrix} 1 & & & & \\ & 3 & & & \\ & & 3 & & \\ & & & 11 & \\ & & & & 27 \end{bmatrix} \mathsf{X}^6 + \begin{bmatrix} 1 & & & & \\ & 3 & & & \\ & & 3 & & \\ & & & 3 & \\ & & & & 3 \end{bmatrix} \mathsf{X}^7 + \begin{bmatrix} 1 & & & & \\ & 3 & & & \\ & & 3 & & \\ & & & 11 & \\ & & & & 27 \end{bmatrix} \mathsf{X}^8.$$

Mediante un cálculo inmediato e independiente por parte de cada usuario tenemos

$$f_1(M) = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 3 & 0 & 0 & 2 \\ 0 & 4 & 1 & 6 & 5 \\ 0 & 8 & 12 & 7 & 14 \\ 16 & 16 & 16 & 20 & 21 \end{bmatrix}, \quad f_2(M) = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 2 \\ 0 & 0 & 1 & 6 & 7 \\ 0 & 0 & 0 & 13 & 6 \\ 16 & 16 & 24 & 8 & 13 \end{bmatrix},$$

$$f_3(M) = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 \\ 0 & 2 & 7 & 6 & 4 \\ 8 & 4 & 6 & 4 & 6 \\ 16 & 16 & 20 & 30 & 27 \end{bmatrix}, \quad f_4(M) = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 3 & 2 \\ 0 & 2 & 5 & 4 & 6 \\ 8 & 8 & 2 & 4 & 6 \\ 16 & 8 & 28 & 26 & 29 \end{bmatrix}.$$

Notemos que $f_i(M)$, con $i = 1, 2, 3, 4$, es un elemento conocido únicamente por el usuario U_i, al ser $f_i(\mathsf{X})$ parte de su clave secreta, pese a ser M público.

Se considera por parte de todos los usuarios inicialmente que $K_0 = N$.

El usuario U_1 obtiene el elemento de $K_1 \in E_2^{(5)}$, calculado como

$$K_1 = f_1(M)^{r_1} K_0 f_1(M)^{s_1} = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 \\ 2 & 0 & 0 & 2 & 1 \\ 4 & 4 & 1 & 1 & 7 \\ 0 & 8 & 4 & 13 & 9 \\ 16 & 8 & 0 & 4 & 9 \end{bmatrix},$$

y se lo envía al usuario U_2.

Entonces el usuario U_2 calcula el elemento

$$K_2 = f_2(M)^{r_2} K_1 f_2(M)^{s_2} = \begin{bmatrix} 1 & 1 & 0 & 1 & 1 \\ 2 & 0 & 0 & 2 & 3 \\ 4 & 4 & 1 & 7 & 6 \\ 0 & 8 & 4 & 9 & 15 \\ 0 & 24 & 8 & 20 & 5 \end{bmatrix},$$

y le envía al usuario U_3 el vector (K_1, K_2), con el que calcula el elemento K_3 como

$$K_3 = f_3(M)^{r_3} K_2 f_3(M)^{s_3} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 2 & 0 & 0 \\ 0 & 2 & 3 & 6 & 0 \\ 8 & 4 & 6 & 8 & 6 \\ 0 & 16 & 4 & 14 & 7 \end{bmatrix},$$

y le envía al usuario U_4 el vector (K_1, K_2, K_3).

A continuación, el usuario U_4 calcula los elementos $L_0^{(4)}, L_1^{(4)}, L_2^{(4)}$ y $L_3^{(4)}$ como

$$L_0^{(4)} = f_4(M)^{r_4} K_0 f_4(M)^{s_4} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 2 & 0 & 0 \\ 0 & 2 & 3 & 2 & 6 \\ 8 & 4 & 6 & 0 & 2 \\ 0 & 16 & 20 & 14 & 23 \end{bmatrix},$$

$$L_1^{(4)} = f_4(M)^{r_4} K_1 f_4(M)^{s_4} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 2 \\ 0 & 2 & 3 & 4 & 7 \\ 8 & 4 & 6 & 4 & 12 \\ 16 & 0 & 28 & 6 & 11 \end{bmatrix},$$

$$L_2^{(4)} = f_4(M)^{r_4} K_2 f_4(M)^{s_4} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 2 & 0 & 0 \\ 0 & 2 & 3 & 2 & 6 \\ 8 & 4 & 6 & 0 & 2 \\ 0 & 16 & 20 & 14 & 7 \end{bmatrix},$$

$$L_3^{(4)} = f_4(M)^{r_4} K_3 f_4(M)^{s_4} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 2 & 0 & 0 \\ 0 & 2 & 3 & 2 & 6 \\ 8 & 4 & 6 & 0 & 2 \\ 0 & 16 & 20 & 14 & 23 \end{bmatrix}.$$

Entonces, el usuario U_4 le envía al usuario U_3 el vector $\left(L_0^{(4)}, L_1^{(4)}, L_2^{(4)}\right)$.

El usuario U_3 calcula los elementos $L_0^{(3)}, L_1^{(3)}$ y $L_2^{(3)}$ como

$$L_0^{(3)} = f_3(M)^{r_3} L_0^{(4)} f_3(M)^{s_3} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 2 & 0 & 0 \\ 0 & 2 & 3 & 2 & 6 \\ 8 & 4 & 6 & 0 & 2 \\ 0 & 16 & 20 & 14 & 7 \end{bmatrix},$$

$$L_1^{(3)} = f_3(M)^{r_3} L_1^{(4)} f_3(M)^{s_3} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 \\ 0 & 2 & 3 & 4 & 7 \\ 8 & 4 & 6 & 4 & 12 \\ 16 & 0 & 28 & 6 & 27 \end{bmatrix},$$

$$L_2^{(3)} = f_3(M)^{r_3} L_2^{(4)} f_3(M)^{s_3} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 2 & 0 & 0 \\ 0 & 2 & 3 & 2 & 6 \\ 8 & 4 & 6 & 0 & 2 \\ 0 & 16 & 20 & 14 & 23 \end{bmatrix},$$

y le envía al usuario U_2 el vector $\left(L_0^{(3)}, L_1^{(3)}\right)$.

A continuación, el usuario U_2 calcula los elementos $L_0^{(2)}$ y $L_1^{(2)}$ como

$$L_0^{(2)} = f_2(M)^{r_2} L_0^{(3)} f_2(M)^{s_2} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 2 \\ 0 & 2 & 3 & 0 & 5 \\ 8 & 4 & 6 & 12 & 8 \\ 16 & 0 & 12 & 6 & 11 \end{bmatrix},$$

$$L_1^{(2)} = f_2(M)^{r_2} L_1^{(3)} f_2(M)^{s_2} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 2 & 0 & 0 \\ 0 & 2 & 3 & 2 & 6 \\ 8 & 4 & 6 & 0 & 2 \\ 0 & 16 & 20 & 14 & 23 \end{bmatrix}.$$

Finalmente, el usuario U_2 envía al usuario U_1 el elemento $L_0^{(2)}$, con lo que el usuario U_1 calcula $L_0^{(1)}$ como

$$L_0^{(1)} = f_1(M)^{r_1} L_0^{(2)} f_1(M)^{s_1} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 2 & 0 & 0 \\ 0 & 2 & 3 & 2 & 6 \\ 8 & 4 & 6 & 0 & 2 \\ 0 & 16 & 20 & 14 & 23 \end{bmatrix}.$$

Notemos, como consecuencia del teorema 4.4, que todos los usuarios comparten el mismo secreto, que es

$$L_0^{(1)} = L_1^{(2)} = L_2^{(3)} = L_3^{(4)} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 2 & 0 & 0 \\ 0 & 2 & 3 & 2 & 6 \\ 8 & 4 & 6 & 0 & 2 \\ 0 & 16 & 20 & 14 & 23 \end{bmatrix}.$$

Supongamos que un nuevo usuario, U_5, quiere unirse (*join*) al sistema anterior. En este caso, el usuario U_4 debe volver a generar una nueva clave privada, naturalmente distinta a la que poseía anteriormente, que denota por $\left(\widehat{r}_4, \widehat{s}_4, \widehat{f}_4(\mathsf{X})\right)$.

La nueva clave privada del usuario U_4 está formada por $\widehat{r}_4 = 7$, $\widehat{s}_4 = 4$ y el

polinomio $\widehat{f_4}(\mathsf{X})$ dado por la expresión

$$\widehat{f_4}(\mathsf{X}) = \begin{bmatrix} 1 & & & & \\ & 3 & & & \\ & & 7 & & \\ & & & 7 & \\ & & & & 7 \end{bmatrix} + \begin{bmatrix} 1 & & & & \\ & 1 & & & \\ & & 5 & & \\ & & & 5 & \\ & & & & 21 \end{bmatrix} \mathsf{X} + \begin{bmatrix} 1 & & & & \\ & 1 & & & \\ & & 5 & & \\ & & & 5 & \\ & & & & 5 \end{bmatrix} \mathsf{X}^2$$
$$+ \begin{bmatrix} 0 & & & & \\ & 0 & & & \\ & & 4 & & \\ & & & 4 & \\ & & & & 20 \end{bmatrix} \mathsf{X}^3.$$

Entonces, el usuario U_4 calcula

$$\widehat{f_4}(M) = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 3 & 2 & 3 & 0 \\ 0 & 0 & 7 & 4 & 5 \\ 0 & 4 & 12 & 5 & 14 \\ 16 & 8 & 0 & 4 & 23 \end{bmatrix}.$$

El nuevo usuario U_5 elige su clave privada formada por $(r_5, s_5, f_5(\mathsf{X}))$, donde $r_5 = 4$, $s_5 = 10$ y el polinomio $f_5(\mathsf{X})$ viene dado por la expresión

$$f_5(\mathsf{X}) = \begin{bmatrix} 0 & & & & \\ & 0 & & & \\ & & 0 & & \\ & & & 0 & \\ & & & & 16 \end{bmatrix} + \begin{bmatrix} 1 & & & & \\ & 1 & & & \\ & & 5 & & \\ & & & 13 & \\ & & & & 29 \end{bmatrix} \mathsf{X} + \begin{bmatrix} 0 & & & & \\ & 2 & & & \\ & & 6 & & \\ & & & 14 & \\ & & & & 30 \end{bmatrix} \mathsf{X}^2.$$

Entonces, el usuario U_5 calcula

$$f_5(M) = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 6 & 5 & 6 & 7 \\ 8 & 8 & 6 & 6 & 4 \\ 0 & 8 & 28 & 6 & 17 \end{bmatrix}.$$

Notemos que ahora el esquema se inicia con el usuario U_4, que calcula

$$K_4 = \widehat{f}_4(M)^{\widehat{r}_4} K_3 \widehat{f}_4(M)^{\widehat{s}_4} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 2 \\ 0 & 6 & 1 & 4 & 1 \\ 8 & 12 & 2 & 12 & 12 \\ 16 & 0 & 20 & 18 & 1 \end{bmatrix},$$

y envía a al usuario U_5 el vector (K_1, K_2, K_3, K_4).

A continuación, el usuario U_5 calcula los elementos $L_0^{(5)}$, $L_1^{(5)}$, $L_2^{(5)}$, $L_3^{(5)}$ y $L_4^{(5)}$ como

$$L_0^{(5)} = f_5(M)^{r_5} K_0 f_5(M)^{s_5} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 2 & 0 & 0 \\ 0 & 2 & 3 & 2 & 6 \\ 8 & 4 & 6 & 0 & 2 \\ 0 & 16 & 20 & 14 & 23 \end{bmatrix},$$

$$L_1^{(5)} = f_5(M)^{r_5} K_1 f_5(M)^{s_5} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 2 \\ 0 & 2 & 3 & 4 & 7 \\ 8 & 4 & 6 & 4 & 12 \\ 16 & 0 & 28 & 6 & 11 \end{bmatrix},$$

$$L_2^{(5)} = f_5(M)^{r_5} K_2 f_5(M)^{s_5} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 2 & 0 & 0 \\ 0 & 2 & 3 & 2 & 6 \\ 8 & 4 & 6 & 0 & 2 \\ 0 & 16 & 20 & 14 & 7 \end{bmatrix},$$

$$L_3^{(5)} = f_5(M)^{r_5} K_3 f_5(M)^{s_5} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 2 & 0 & 0 \\ 0 & 2 & 3 & 2 & 6 \\ 8 & 4 & 6 & 0 & 2 \\ 0 & 16 & 20 & 14 & 23 \end{bmatrix},$$

$$L_4^{(5)} = f_5(M)^{r_5} K_4 f_5(M)^{s_5} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 2 \\ 0 & 6 & 1 & 0 & 3 \\ 8 & 12 & 2 & 4 & 0 \\ 16 & 0 & 4 & 18 & 1 \end{bmatrix},$$

y envía al usuario U_4 el vector $\left(L_0^{(5)}, L_1^{(5)}, L_2^{(5)}, L_3^{(5)}\right)$. Entonces, el usuario U_4 calcula los elementos $L_0^{(4)}$, $L_1^{(4)}$, $L_2^{(4)}$ y $L_3^{(4)}$ como

$$L_0^{(4)} = \widehat{f}_4(M)^{\widehat{r}_4} L_0^{(5)} \widehat{f}_4(M)^{\widehat{s}_4} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 2 \\ 0 & 6 & 1 & 0 & 3 \\ 8 & 12 & 2 & 4 & 0 \\ 16 & 0 & 4 & 18 & 1 \end{bmatrix},$$

$$L_1^{(4)} = \widehat{f}_4(M)^{\widehat{r}_4} L_1^{(5)} \widehat{f}_4(M)^{\widehat{s}_4} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 2 & 0 & 0 \\ 0 & 6 & 1 & 6 & 6 \\ 8 & 12 & 2 & 0 & 14 \\ 0 & 16 & 28 & 10 & 5 \end{bmatrix},$$

$$L_2^{(4)} = \widehat{f}_4(M)^{\widehat{r}_4} L_2^{(5)} \widehat{f}_4(M)^{\widehat{s}_4} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 2 \\ 0 & 6 & 1 & 0 & 3 \\ 8 & 12 & 2 & 4 & 0 \\ 16 & 0 & 4 & 18 & 17 \end{bmatrix},$$

$$L_3^{(4)} = \widehat{f}_4(M)^{\widehat{r}_4} L_3^{(5)} \widehat{f}_4(M)^{\widehat{s}_4} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 2 \\ 0 & 6 & 1 & 0 & 3 \\ 8 & 12 & 2 & 4 & 0 \\ 16 & 0 & 4 & 18 & 1 \end{bmatrix}.$$

Ahora, el usuario U_4 envía al usuario U_3 el vector $\left(L_0^{(4)}, L_1^{(4)}, L_2^{(4)}\right)$. Entonces, el usuario U_3 calcula el vector $\left(L_0^{(3)}, L_1^{(3)}, L_2^{(3)}\right)$ y envía al usuario U_2 el vector $\left(L_0^{(3)}, L_1^{(3)}\right)$. Ahora, el usuario U_2 calcula el vector $\left(L_0^{(2)}, L_1^{(2)}\right)$. Para terminar, el usuario U_2 envía al usuario U_1 únicamente el elemento $L_0^{(2)}$, con el fin de que U_1 calcule $L_0^{(1)}$.

Como consecuencia del teorema 4.4, todos los usuarios comparten el mismo elemento secreto, que es

$$L_0^{(1)} = L_1^{(2)} = L_2^{(3)} = L_3^{(4)} = L_4^{(5)} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 2 \\ 0 & 6 & 1 & 0 & 3 \\ 8 & 12 & 2 & 4 & 0 \\ 16 & 0 & 4 & 18 & 1 \end{bmatrix}.$$

A continuación, supongamos por ejemplo que el usuario U_3 quiere abandonar (*leave*) el sistema anterior, tras la unión del usuario U_5. Entonces, el usuario U_2 debe cambiar su clave privada. La nueva clave privada elegida por U_2 es $\left(\widehat{r}_2, \widehat{s}_2, \widehat{f}_2(\mathsf{X})\right)$, donde $\widehat{r}_2 = 3$, $\widehat{s}_2 = 6$ y el polinomio $\widehat{f}_2(\mathsf{X})$ viene dado por

$$\widehat{f}_2(\mathsf{X}) = \begin{bmatrix} 0 & & & & \\ & 2 & & & \\ & & 2 & & \\ & & & 2 & \\ & & & & 2 \end{bmatrix} + \begin{bmatrix} 0 & & & & \\ & 0 & & & \\ & & 4 & & \\ & & & 12 & \\ & & & & 28 \end{bmatrix} \mathsf{X} + \begin{bmatrix} 0 & & & & \\ & 0 & & & \\ & & 4 & & \\ & & & 12 & \\ & & & & 28 \end{bmatrix} \mathsf{X}^2$$
$$+ \begin{bmatrix} 0 & & & & \\ & 2 & & & \\ & & 2 & & \\ & & & 2 & \\ & & & & 18 \end{bmatrix} \mathsf{X}^3 + \begin{bmatrix} 0 & & & & \\ & 0 & & & \\ & & 4 & & \\ & & & 12 & \\ & & & & 28 \end{bmatrix} \mathsf{X}^4 + \begin{bmatrix} 1 & & & & \\ & 3 & & & \\ & & 7 & & \\ & & & 7 & \\ & & & & 23 \end{bmatrix} \mathsf{X}^5.$$

Ahora, el usuario U_2 calcula

$$\widehat{f}_2(M) = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 2 & 2 & 0 & 2 \\ 0 & 2 & 5 & 4 & 7 \\ 8 & 4 & 6 & 14 & 4 \\ 0 & 0 & 12 & 6 & 21 \end{bmatrix}.$$

Entonces, el usuario U_2 calcula un nuevo elemento K_2 como

$$K_2 = \widehat{f}_2(M)^{\widehat{r}_2} K_1 \widehat{f}_2(M)^{\widehat{s}_2} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 2 & 0 & 0 \\ 0 & 2 & 7 & 2 & 6 \\ 8 & 4 & 14 & 0 & 2 \\ 0 & 16 & 4 & 6 & 3 \end{bmatrix},$$

y envía al usuario U_4 el vector (K_1, K_2).

A continuación, el usuario U_4 calcula el elemento K_3 como

$$K_3 = \widehat{f_4}(M)^{\widehat{r_4}} K_2 \widehat{f_4}(M)^{\widehat{s_4}} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 2 \\ 0 & 6 & 5 & 0 & 7 \\ 8 & 12 & 10 & 4 & 8 \\ 16 & 0 & 20 & 26 & 21 \end{bmatrix},$$

y envía el vector (K_1, K_2, K_3) al usuario U_5, que calcula los elementos $L_0^{(5)}$, $L_1^{(5)}$, $L_2^{(5)}$ y $L_3^{(5)}$ como

$$L_0^{(5)} = f_5(M)^{r_5} K_0 f_5(M)^{s_5} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 2 & 0 & 0 \\ 0 & 2 & 3 & 2 & 6 \\ 8 & 4 & 6 & 0 & 2 \\ 0 & 16 & 20 & 14 & 23 \end{bmatrix},$$

$$L_1^{(5)} = f_5(M)^{r_5} K_1 f_5(M)^{s_5} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 2 \\ 0 & 2 & 3 & 4 & 7 \\ 8 & 4 & 6 & 4 & 12 \\ 16 & 0 & 28 & 6 & 11 \end{bmatrix},$$

$$L_2^{(5)} = f_5(M)^{r_5} K_2 f_5(M)^{s_5} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 2 & 0 & 0 \\ 0 & 2 & 7 & 6 & 4 \\ 8 & 4 & 14 & 8 & 6 \\ 0 & 16 & 20 & 6 & 3 \end{bmatrix},$$

$$L_3^{(5)} = f_5(M)^{r_5} K_3 f_5(M)^{s_5} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 2 \\ 0 & 6 & 5 & 4 & 1 \\ 8 & 12 & 10 & 12 & 4 \\ 16 & 0 & 4 & 26 & 5 \end{bmatrix}.$$

Posteriormente, el usuario U_5 envía el vector $\left(L_0^{(5)}, L_1^{(5)}, L_2^{(5)}\right)$ al usuario U_4 y éste calcula los elementos $L_0^{(4)}$, $L_1^{(4)}$ y $L_2^{(4)}$ como

$$L_0^{(4)} = \widehat{f}_4(M)^{\widehat{r}_4} L_0^{(5)} \widehat{f}_4(M)^{\widehat{s}_4} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 2 \\ 0 & 6 & 1 & 0 & 3 \\ 8 & 12 & 2 & 4 & 0 \\ 16 & 0 & 4 & 18 & 1 \end{bmatrix},$$

$$L_1^{(4)} = \widehat{f}_4(M)^{\widehat{r}_4} L_1^{(5)} \widehat{f}_4(M)^{\widehat{s}_4} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 2 & 0 & 0 \\ 0 & 6 & 1 & 6 & 6 \\ 8 & 12 & 2 & 0 & 14 \\ 0 & 16 & 28 & 10 & 5 \end{bmatrix},$$

$$L_2^{(4)} = \widehat{f}_4(M)^{\widehat{r}_4} L_2^{(5)} \widehat{f}_4(M)^{\widehat{s}_4} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 2 \\ 0 & 6 & 5 & 4 & 1 \\ 8 & 12 & 10 & 12 & 4 \\ 16 & 0 & 4 & 26 & 5 \end{bmatrix}.$$

Ahora, el usuario U_4 envía el vector $\left(L_0^{(4)}, L_1^{(4)}\right)$ al usuario U_2 y éste calcula $L_0^{(2)}$ y $L_1^{(2)}$ como

$$L_0^{(2)} = \widehat{f}_2(M)^{\widehat{r}_2} L_0^{(4)} \widehat{f}_2(M)^{\widehat{s}_2} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 2 & 0 & 0 \\ 0 & 6 & 5 & 6 & 2 \\ 8 & 12 & 10 & 0 & 14 \\ 0 & 16 & 12 & 18 & 25 \end{bmatrix},$$

$$L_1^{(2)} = \widehat{f}_2(M)^{\widehat{r}_2} L_1^{(4)} \widehat{f}_2(M)^{\widehat{s}_2} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 2 \\ 0 & 6 & 5 & 4 & 1 \\ 8 & 12 & 10 & 12 & 4 \\ 16 & 0 & 4 & 26 & 5 \end{bmatrix}.$$

Para finalizar, el usuario U_2 envía al usuario U_1 el elemento $L_0^{(2)}$ y éste calcula $L_0^{(1)}$ como

$$L_0^{(1)} = f_1(M)^{r_1} L_0^{(2)} f_1(M)^{s_1} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 2 \\ 0 & 6 & 5 & 4 & 1 \\ 8 & 12 & 10 & 12 & 4 \\ 16 & 0 & 4 & 26 & 5 \end{bmatrix}.$$

Nuevamente, como consecuencia del teorema 4.4, todos los usuarios que siguen en el sistema comparten el mismo elemento secreto, que es

$$L_0^{(1)} = L_1^{(2)} = L_2^{(4)} = L_3^{(5)} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 2 \\ 0 & 6 & 5 & 4 & 1 \\ 8 & 12 & 10 & 12 & 4 \\ 16 & 0 & 4 & 26 & 5 \end{bmatrix}.$$

■

4.3.2 Esquema de multidifusión en bloque

Antes de mostrar el funcionamiento del siguiente esquema de multidifusión, necesitamos introducir la siguiente notación para describir y simplificar ciertos sumatorios.

$$\sigma(j,1,i) = \sum_{j=1}^{i-1} j \qquad \text{y} \qquad \delta(j,1,i,l) = \sum_{\substack{j=1 \\ j \neq i-l}}^{i-1} j. \tag{4.19}$$

Protocolo 4.5: *Consideramos que se comparten los elementos públicos, $M \in R$ y $K_0 = N \in R \setminus Z(R)$. Cada usuario U_i, para $i = 1, 2, \ldots, h$ elige un polinomio $f_i(\mathsf{X}) \in Z(R)[\mathsf{X}]$ y un par de enteros positivos r_i y s_i. De esta forma la clave secreta para el usuario U_i viene determinada por la terna $(r_i, s_i, f_i(\mathsf{X}))$.*

(a) *El usuario U_1 calcula el elemento $K_1 \in R$ dado por la expresión*

$$K_1 = f_1(M)^{r_1} K_0 f_1(M)^{s_1}. \tag{4.20}$$

El usuario U_1 envía el elemento K_1 al usuario U_2.

(b) *El usuario U_2 calcula los elementos K_2 y K_3 de R*

$$\begin{aligned} K_2 &= f_2(M)^{r_2} K_0 f_2(M)^{s_2}, \\ K_3 &= f_2(M)^{r_2} K_1 f_2(M)^{s_2}. \end{aligned} \tag{4.21}$$

El usuario U_2 envía el vector (K_1, K_2, K_3) al usuario U_3.

(c) *El usuario U_3 calcula los elementos K_4, K_5 y K_6 de R como*

$$\begin{aligned} K_4 &= f_3(M)^{r_3} K_1 f_3(M)^{s_3}, \\ K_5 &= f_3(M)^{r_3} K_2 f_3(M)^{s_3}, \\ K_6 &= f_3(M)^{r_3} K_3 f_3(M)^{s_3}. \end{aligned} \tag{4.22}$$

El usuario U_3 envía al usuario U_4 el vector (K_3, K_4, K_5, K_6).

(d) *En general, con la notación de la expresión (4.19), para $i = 4, 5, \ldots, h-1$, el usuario U_i calcula los elementos de R como*

$$\begin{aligned} K_{i+\delta(j,1,i,l)} &= f_i(M)^{r_i} K_{\delta(j,1,i,l)} f_i(M)^{s_i}, \quad \text{para } l = 1, 2, 3, \ldots, i-1, \\ K_{i+\sigma(j,1,i)} &= f_i(M)^{r_i} K_{\sigma(j,1,i)} f_i(M)^{s_i}. \end{aligned} \tag{4.23}$$

El usuario U_i envía al usuario U_{i+1} el $(i+1)$-vector de elementos de R

$$\Big(K_{i-1+\delta(j,1,i,1)}, K_{i+\delta(j,1,i,1)}, K_{i+\delta(j,1,i,2)}, \ldots, K_{i+\delta(j,1,i,i-1)}, K_{\sigma(j,1,i+1)}\Big).$$

(e) *Cuando el usuario U_h recibe el h-vector*

$$\Big(K_{h-2+\delta(j,1,h-1,1)}, K_{h-1+\delta(j,1,h-1,1)}, K_{h-1+\delta(j,1,h-1,2)}, \ldots, K_{h-1+\delta(j,1,h-1,h-2)}, K_{\sigma(j,1,h)}\Big), \tag{4.24}$$

calcula los siguientes elementos del anillo R

$$L_1^{(h)} = f_h(M)^{r_h} K_{h-2+\delta(j,1,h-1,1)} f_h(M)^{s_h}, \tag{4.25}$$

$$\begin{aligned} L_l^{(h)} &= f_h(M)^{r_h} K_{h-1+\delta(j,1,h-1,l-1)} f_h(M)^{s_h}, \\ &= f_h(M)^{r_h} K_{\delta(j,1,h,l)} f_h(M)^{s_h}, \quad \textit{para } l = 2, 3, \ldots, h-1, \end{aligned} \tag{4.26}$$

$$L_h^{(h)} = f_h(M)^{r_h} K_{\sigma(j,1,h)} f_h(M)^{s_h}. \tag{4.27}$$

El último usuario U_h, envía a cada uno de los anteriores usuarios de forma simultánea el $(h-1)$-vector $\left(L_1^{(h)}, L_2^{(h)}, \ldots, L_{h-1}^{(h)}\right)$ de elementos de R.

(f) *Finalmente, cuando el usuario U_i, for $i = 1, 2, \ldots, h-1$, recibe el $(h-1)$-vector $\left(L_1^{(h)}, L_2^{(h)}, \ldots, L_{h-1}^{(h)}\right)$, éste toma la $(h-i)$-componente del vector, $L_{h-i}^{(h)}$, y calcula el elemento*

$$S_i = f_i(M)^{r_i} L_{h-i}^{(h)} f_i(M)^{s_i}. \tag{4.28}$$

Por último y por cuestiones de notación, el usuario U_h denota por S_h el elemento $L_h^{(h)}$.

El siguiente teorema establece que la clave secreta compartida entre todos los usuarios del sistema es la misma, $S_h = L_h^{(h)}$.

Teorema 4.5: *Con la notación del esquema 4.5, todos los usuarios comparten la misma clave secreta,*

$$S_1 = S_2 = \cdots = S_{h-1} = S_h = L_h^{(h)}. \tag{4.29}$$

DEMOSTRACIÓN: Suponemos que el esquema de intercambio está formado por los

usuarios $U_1, U_2, \ldots, U_h$. Con la notación utilizada en el esquema 4.5 y como consecuencia de las expresiones (4.20)–(4.23), (4.25)–(4.27) y (4.10), resulta que

$$L_{h-i}^{(h)} = \left(\prod_{\substack{j=1 \\ j \neq i}}^{h} f_j(M)^{r_j} \right) K_0 \left(\prod_{\substack{j=1 \\ j \neq i}}^{h} f_j(M)^{s_j} \right). \tag{4.30}$$

A continuación, como consecuencia de las expresiones (4.28), (4.30) y (4.10) tenemos que

$$S_i = \left(\prod_{j=1}^{h} f_j(M)^{r_j} \right) K_0 \left(\prod_{j=1}^{h} f_j(M)^{s_j} \right),$$

con lo que queda demostrada la expresión (4.29). □

Notemos que la principal ventaja que presenta este esquema respecto al esquema 4.4, es que se reducen considerablemente el número de mensajes y rondas de intercambio de información entre los usuarios; más concretamente, son necesarios h mensajes y rondas.

Cuando un nuevo usuario U_{h+1} pretende unirse al esquema, operación *join*, es necesario hacer un cambio de claves para preservar el secreto compartido. Para ello debemos suponer que el usuario U_h ha almacenado el h-vector de elementos de R dado por la expresión (4.24). Entonces, la operación de unión al sistema, se lleva a cabo según los siguientes pasos:

(a) El usuario U_h genera una nueva clave secreta, formada por un nuevo polinomio $\widehat{f}_h(\mathsf{X}) \in Z(R)$ y dos nuevos enteros positivos $\widehat{r}_h$ y $\widehat{s}_h$. Con su nueva clave secreta, el usuario U_h calcula los elementos de R dados por las expresiones

$$K_{h+\delta(j,1,h,l)} = \widehat{f}_h(M)^{\widehat{r}_h} K_{\delta(j,1,h,l)} \widehat{f}_h(M)^{\widehat{s}_h}, \quad \text{para } l = 2, 3, \ldots, h-1,$$
$$K_{h+\sigma(j,1,h)} = \widehat{f}_h(M)^{\widehat{r}_h} K_{\sigma(j,1,h)} \widehat{f}_h(M)^{\widehat{s}_h}.$$

A continuación, el usuario U_h envía al nuevo usuario U_{h+1} el $(h+1)$-vector de elementos de R,

$$u\Big(K_{h-1+\delta(j,1,h,1)}, K_{h+\delta(j,1,h,1)}, K_{h+\delta(j,1,h,2)}, \ldots, K_{h+\delta(j,1,h,h-1)}, K_{\sigma(j,1,h+1)}\Big).$$

(b) El usuario U_{h+1}, tal y como anteriormente hizo el usuario U_h, calcula los elementos de R,

$$\begin{aligned} L_1^{(h+1)} &= f_{h+1}(M)^{r_{h+1}} K_{h-1+\delta(j,1,h,1)} f_{h+1}(M)^{s_{h+1}}, \\ L_l^{(h+1)} &= f_{h+1}(M)^{r_{h+1}} K_{h+\delta(j,1,h,l-1)} f_{h+1}(M)^{s_{h+1}}, \\ &= f_{h+1}(M)^{r_{h+1}} K_{\delta(j,1,h+1,l)} f_{h+1}(M)^{s_{h+1}}, \quad \text{para } l = 2,3,\ldots,h, \\ L_{h+1}^{(h+1)} &= f_{h+1}(M)^{r_{h+1}} K_{\sigma(j,1,h+1)} f_{h+1}(M)^{s_{h+1}}. \end{aligned}$$

(c) El usuario U_{h+1} envía de forma simultánea a cada uno de los usuarios del esquema el h-vector de elementos de R

$$\left(L_1^{(h+1)}, L_2^{(h+1)}, \ldots, L_h^{(h+1)}\right). \tag{4.31}$$

(d) Por último, cuando cada usuario U_i, para $i = 1,2,\ldots,h$, recibe el h-vector dado por la expresión (4.31), toma la $(h+1-i)$ componente $L_{h+1-i}^{(h+1)}$, y calcula el nuevo elemento $\widehat{S}_i$ como

$$\widehat{S}_i = f_i(M)^{r_i} L_{h+1-i}^{(h+1)} f_i(M)^{s_i}, \quad \text{para } i = 1,2,\ldots,h.$$

El usuario U_{h+1} denota por $\widehat{S}_h$ el elemento $L_{h+1}^{(h+1)}$, esto es, $\widehat{S}_{h+1} = L_{h+1}^{(h+1)}$.

Como consecuencia del teorema 4.5, el nuevo secreto es compartido por todos los usuarios del esquema

$$\widehat{S}_1 = \widehat{S}_2 = \cdots = \widehat{S}_h = \widehat{S}_{h+1}.$$

Supongamos, como viene siendo habitual, que el sistema está formado por los usuarios $U_1, U_2, \ldots, U_h$. Si suponemos que el usuario U_i, para algún $i \in \{1,2,\ldots,h\}$, desea abandonar el sistema, operación *leave*, es necesario un cambio de claves para preservar el secreto compartido.

Recordemos que el usuario U_h posee el h-vector de elementos de R dado por la expresión (4.24). Tal y como ocurría con la operación de unión al sistema, el usuario U_h debe generar una nueva clave secreta, es decir, elige un nuevo polinomio $\widehat{f}_h(\mathsf{X}) \in Z(R)$ y dos nuevos enteros positivos $\widehat{r}_h$ y $\widehat{s}_h$. Entonces, el usuario U_h calcula los elementos de R,

$$L_1^{(h)} = \widehat{f}_h(M)^{\widehat{r}_h} K_{h-2+\delta(j,1,h-1,1)} \widehat{f}_h(M)^{\widehat{s}_h},$$

$$\begin{aligned} L_l^{(h)} &= \widehat{f}_h(M)^{\widehat{r}_h} K_{h-1+\delta(j,1,h-1,l-1)} \widehat{f}_h(M)^{\widehat{s}_h}, \\ &= \widehat{f}_h(M)^{\widehat{r}_h} K_{\delta(j,1,h,l)} \widehat{f}_h(M)^{\widehat{s}_h}, \quad \text{para } l = 2, 3, \ldots, h-1, \\ L_h^{(h)} &= \widehat{f}_h(M)^{\widehat{r}_h} K_{\sigma(j,1,h)} \widehat{f}_h(M)^{\widehat{s}_h}. \end{aligned}$$

Notemos que se utilizan las expresiones (4.25), (4.26), (4.27) para calcular $L_l^{(h)}$, de forma que los elementos $f_l(M)$, r_l y s_l son reemplazados por $\widehat{f}_l(M)$, $\widehat{r}_l$ y $\widehat{s}_l$ para $l = 1, 2, \ldots, h$, respectivamente.

Para finalizar, el usuario U_h envía de forma simultánea a todos los usuarios, excepto al usuario U_i que abandonó el sistema, el $(h-1)$-vector $\left(L_1^{(h)}, L_2^{(h)}, \ldots, L_{h-1}^{(h)}\right)$ de elementos de R, de forma que cada usuario calcula de forma independiente la nueva clave secreta como en el paso (f) del esquema 4.5.

Notemos que en el caso de que sea el usuario U_h el que decide abandonar el sistema, basta con que el usuario U_{h-1} cambie su clave secreta, para lo cual considera un nuevo polinomio y un nuevo par de enteros positivos, de forma que pasa a actuar como el nuevo último usuario del sistema, tal y como lo hacía el usuario U_h.

A modo de ejemplo del esquema de multidifusión 4.5 sobre ${E_p}^{(m)}$, consideramos un ejemplo similar al desarrollado en el esquema 4.4, donde mostramos claramente las semejanzas y diferencias que presentan los dos esquemas de intercambio. Para ello consideramos el anillo $E_2^{(5)}$. Notemos que para un caso real necesitamos considerar parámetros más elevados tanto para el primo p como para el entero m, para evitar posibles ataques por fuerza bruta al sistema.

Supongamos que el esquema de multidifusión está formado por cuatro usuarios y que éstos comparten dos elementos. Podemos suponer que se tratan de los mismos elementos elegidos en el ejemplo propuesto para el esquema 4.4, dados por la expresión (4.4).

$$M = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 2 & 3 & 2 & 7 \\ 8 & 0 & 2 & 14 & 0 \\ 0 & 8 & 4 & 2 & 23 \end{bmatrix} \in E_2^{(5)} \quad \text{y} \quad N = \begin{bmatrix} 1 & 1 & 0 & 1 & 1 \\ 2 & 0 & 0 & 2 & 3 \\ 4 & 0 & 5 & 1 & 2 \\ 0 & 0 & 0 & 7 & 15 \\ 0 & 8 & 0 & 0 & 5 \end{bmatrix} \in E_2^{(5)} \setminus Z\left(E_2^{(5)}\right).$$

Cada uno de los usuarios del esquema, U_i con $i = 1, 2, 3, 4$, elige como clave privada la terna $(r_i, s_i, f_i(\mathsf{X}))$, con los enteros positivos

$$(r_1, r_2, r_3, r_4) = (10, 5, 6, 11), (s_1, s_2, s_3, s_4) = (5, 14, 16, 12),$$

y los polinomios $f_i(\mathsf{X}) \in Z\left(E_2^{(5)}\right)$ con $i = 1, 2, 3, 4$, dados por las expresiones

$$f_1(\mathsf{X}) = \begin{bmatrix} 1 & & & & \\ & 3 & & & \\ & & 3 & & \\ & & & 11 & \\ & & & & 11 \end{bmatrix} + \begin{bmatrix} 0 & & & & \\ & 2 & & & \\ & & 2 & & \\ & & & 10 & \\ & & & & 26 \end{bmatrix} \mathsf{X}^2 + \begin{bmatrix} 1 & & & & \\ & 1 & & & \\ & & 1 & & \\ & & & 1 & \\ & & & & 17 \end{bmatrix} \mathsf{X}^3$$
$$+ \begin{bmatrix} 1 & & & & \\ & 1 & & & \\ & & 5 & & \\ & & & 13 & \\ & & & & 29 \end{bmatrix} \mathsf{X}^4,$$

$$f_2(\mathsf{X}) = \begin{bmatrix} 1 & & & & \\ & 1 & & & \\ & & 1 & & \\ & & & 9 & \\ & & & & 25 \end{bmatrix} + \begin{bmatrix} 0 & & & & \\ & 2 & & & \\ & & 2 & & \\ & & & 10 & \\ & & & & 26 \end{bmatrix} \mathsf{X}^2 + \begin{bmatrix} 1 & & & & \\ & 3 & & & \\ & & 7 & & \\ & & & 7 & \\ & & & & 23 \end{bmatrix} \mathsf{X}^3$$
$$+ \begin{bmatrix} 0 & & & & \\ & 2 & & & \\ & & 6 & & \\ & & & 6 & \\ & & & & 6 \end{bmatrix} \mathsf{X}^4 + \begin{bmatrix} 0 & & & & \\ & 2 & & & \\ & & 6 & & \\ & & & 6 & \\ & & & & 22 \end{bmatrix} \mathsf{X}^5 + \begin{bmatrix} 1 & & & & \\ & 1 & & & \\ & & 5 & & \\ & & & 5 & \\ & & & & 21 \end{bmatrix} \mathsf{X}^6,$$

$$f_3(\mathsf{X}) = \begin{bmatrix} 0 & & & & \\ & 0 & & & \\ & & 0 & & \\ & & & 0 & \\ & & & & 16 \end{bmatrix} + \begin{bmatrix} 0 & & & & \\ & 2 & & & \\ & & 2 & & \\ & & & 2 & \\ & & & & 2 \end{bmatrix} \mathsf{X} + \begin{bmatrix} 1 & & & & \\ & 1 & & & \\ & & 1 & & \\ & & & 1 & \\ & & & & 17 \end{bmatrix} \mathsf{X}^2,$$

$$f_4(\mathsf{X}) = \begin{bmatrix} 0 & & & & \\ & 2 & & & \\ & & 2 & & \\ & & & 10 & \\ & & & & 10 \end{bmatrix} + \begin{bmatrix} 1 & & & & \\ & 1 & & & \\ & & 1 & & \\ & & & 1 & \\ & & & & 17 \end{bmatrix} \mathsf{X} + \begin{bmatrix} 1 & & & & \\ & 3 & & & \\ & & 3 & & \\ & & & 11 & \\ & & & & 27 \end{bmatrix} \mathsf{X}^2$$
$$+ \begin{bmatrix} 1 & & & & \\ & 3 & & & \\ & & 7 & & \\ & & & 7 & \\ & & & & 23 \end{bmatrix} \mathsf{X}^3 + \begin{bmatrix} 0 & & & & \\ & 0 & & & \\ & & 4 & & \\ & & & 4 & \\ & & & & 4 \end{bmatrix} \mathsf{X}^4 + \begin{bmatrix} 1 & & & & \\ & 3 & & & \\ & & 3 & & \\ & & & 11 & \\ & & & & 11 \end{bmatrix} \mathsf{X}^5$$
$$+ \begin{bmatrix} 1 & & & & \\ & 3 & & & \\ & & 3 & & \\ & & & 11 & \\ & & & & 27 \end{bmatrix} \mathsf{X}^6 + \begin{bmatrix} 1 & & & & \\ & 3 & & & \\ & & 3 & & \\ & & & 3 & \\ & & & & 3 \end{bmatrix} \mathsf{X}^7 + \begin{bmatrix} 1 & & & & \\ & 3 & & & \\ & & 3 & & \\ & & & 11 & \\ & & & & 27 \end{bmatrix} \mathsf{X}^8.$$

De forma independiente, cada uno de los usuarios del sistema calcula respectivamente

$$f_1(M) = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 3 & 0 & 0 & 2 \\ 0 & 4 & 1 & 6 & 5 \\ 0 & 8 & 12 & 7 & 14 \\ 16 & 16 & 16 & 20 & 21 \end{bmatrix}, \quad f_2(M) = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 2 \\ 0 & 0 & 1 & 6 & 7 \\ 0 & 0 & 0 & 13 & 6 \\ 16 & 16 & 24 & 8 & 13 \end{bmatrix},$$

$$f_3(M) = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 \\ 0 & 2 & 7 & 6 & 4 \\ 8 & 4 & 6 & 4 & 6 \\ 16 & 16 & 20 & 30 & 27 \end{bmatrix}, \quad f_4(M) = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 3 & 2 \\ 0 & 2 & 5 & 4 & 6 \\ 8 & 8 & 2 & 4 & 6 \\ 16 & 8 & 28 & 26 & 29 \end{bmatrix}.$$

Notemos que pese a ser M un elemento público, compartido por todos los usuarios del sistema, $f_i(M)$ para $i = 1, 2, 3, 4$, es un elemento conocido sólo por el usuario i-ésimo del sistema. Observemos también que $K_0 = N$.

El usuario U_1 obtiene el elemento de $K_1 \in E_2^{(5)}$, calculado como

$$K_1 = f_1(M)^{r_1} K_0 f_1(M)^{s_1} = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 \\ 2 & 0 & 0 & 2 & 1 \\ 4 & 4 & 1 & 1 & 7 \\ 0 & 8 & 4 & 13 & 9 \\ 16 & 8 & 0 & 4 & 9 \end{bmatrix},$$

y se lo envía al usuario U_2.

Entonces, el usuario U_2 calcula los elementos K_2 y K_3 como

$$K_2 = f_2(M)^{r_2} K_0 f_2(M)^{s_2} = \begin{bmatrix} 1 & 1 & 0 & 1 & 1 \\ 2 & 0 & 0 & 2 & 1 \\ 4 & 0 & 5 & 7 & 1 \\ 0 & 0 & 0 & 3 & 5 \\ 16 & 24 & 8 & 0 & 9 \end{bmatrix},$$

$$K_3 = f_2(M)^{r_2} K_1 f_2(M)^{s_2} = \begin{bmatrix} 1 & 1 & 0 & 1 & 1 \\ 2 & 0 & 0 & 2 & 3 \\ 4 & 4 & 1 & 7 & 6 \\ 0 & 8 & 4 & 9 & 15 \\ 0 & 24 & 8 & 4 & 5 \end{bmatrix},$$

y el usuario U_2 le envía al usuario U_3 el vector (K_1, K_2, K_3).

A continuación, el usuario U_3 calcula los elementos K_4, K_5 y K_6 como

$$K_4 = f_3(M)^{r_3} K_1 f_3(M)^{s_3} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 2 \\ 0 & 2 & 3 & 0 & 1 \\ 8 & 4 & 6 & 12 & 0 \\ 16 & 0 & 12 & 6 & 27 \end{bmatrix},$$

$$K_5 = f_3(M)^{r_3} K_2 f_3(M)^{s_3} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 2 \\ 0 & 2 & 3 & 4 & 7 \\ 8 & 4 & 6 & 4 & 12 \\ 16 & 0 & 28 & 6 & 11 \end{bmatrix},$$

$$K_6 = f_3(M)^{r_3} K_3 f_3(M)^{s_3} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 2 & 0 & 0 \\ 0 & 2 & 3 & 6 & 0 \\ 8 & 4 & 6 & 8 & 6 \\ 0 & 16 & 4 & 14 & 7 \end{bmatrix},$$

y envía el vector (K_3, K_4, K_5, K_6) al usuario U_4.

El usuario U_4, con los elementos recibidos, calcula los elementos $L_1^{(4)}$, $L_2^{(4)}$, $L_3^{(4)}$ y $L_4^{(4)}$ como

$$L_1^{(4)} = f_4(M)^{r_4} K_3 f_4(M)^{s_4} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 2 & 0 & 0 \\ 0 & 2 & 3 & 2 & 6 \\ 8 & 4 & 6 & 0 & 2 \\ 0 & 16 & 20 & 14 & 7 \end{bmatrix},$$

$$L_2^{(4)} = f_4(M)^{r_4} K_4 f_4(M)^{s_4} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 2 \\ 0 & 2 & 3 & 4 & 7 \\ 8 & 4 & 6 & 4 & 12 \\ 16 & 0 & 28 & 6 & 27 \end{bmatrix},$$

$$L_3^{(4)} = f_4(M)^{r_4} K_5 f_4(M)^{s_4} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 2 \\ 0 & 2 & 3 & 0 & 5 \\ 8 & 4 & 6 & 12 & 8 \\ 16 & 0 & 12 & 6 & 11 \end{bmatrix},$$

$$L_4^{(4)} = f_4(M)^{r_4} K_6 f_4(M)^{s_4} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 2 & 0 & 0 \\ 0 & 2 & 3 & 2 & 6 \\ 8 & 4 & 6 & 0 & 2 \\ 0 & 16 & 20 & 14 & 23 \end{bmatrix}.$$

Por último, el usuario U_4 considera $S_4 = L_4^{(4)}$ y envía a todos los usuarios del sistema el vector $\left(L_1^{(4)}, L_2^{(4)}, L_3^{(4)}\right)$.

El usuario U_2, después de recibir el vector anterior del usuario U_4, utiliza la tercera componente, $L_3^{(4)}$, para calcular S_1 como

$$S_1 = f_1(M)^{r_1} L_3^{(4)} f_1(M)^{s_1} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 2 & 0 & 0 \\ 0 & 2 & 3 & 2 & 6 \\ 8 & 4 & 6 & 0 & 2 \\ 0 & 16 & 20 & 14 & 23 \end{bmatrix}.$$

Por su parte, el usuario U_2 utiliza la segunda componente del vector recibido,

$L_2^{(4)}$, para calcular S_2 como

$$S_2 = f_2(M)^{r_2} L_2^{(4)} f_2(M)^{s_2} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 2 & 0 & 0 \\ 0 & 2 & 3 & 2 & 6 \\ 8 & 4 & 6 & 0 & 2 \\ 0 & 16 & 20 & 14 & 23 \end{bmatrix}.$$

Por último, el usuario U_1 utiliza la primera componente, $L_1^{(4)}$, del vector recibido para calcular S_3 como

$$S_3 = f_3(M)^{r_3} L_1^{(4)} f_3(M)^{s_3} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 2 & 0 & 0 \\ 0 & 2 & 3 & 2 & 6 \\ 8 & 4 & 6 & 0 & 2 \\ 0 & 16 & 20 & 14 & 23 \end{bmatrix}.$$

Es inmediato comprobar, como consecuencia del teorema 4.5, que el secreto compartido por todos los usuarios del sistema es

$$S_1 = S_2 = S_3 = S_4 = L_4^{(4)}.$$

Observemos que el número de mensajes y rondas de envío es menor en este ejemplo si lo comparamos con el ejemplo del esquema 4.4 visto en la sección anterior.

Supongamos que un nuevo usuario, U_5, quiere unirse al sistema anterior. En este caso, el usuario U_4 debe cambiar su clave privada por una nueva $\left(\widehat{r}_4, \widehat{s}_4, \widehat{f}_4(\mathsf{X})\right)$. Con $\widehat{r}_4 = 7$, $\widehat{s}_4 = 4$ y el polinomio $\widehat{f}_4(\mathsf{X})$ dado por la expresión

$$\widehat{f}_4(\mathsf{X}) = \begin{bmatrix} 1 & & & & \\ & 3 & & & \\ & & 7 & & \\ & & & 7 & \\ & & & & 7 \end{bmatrix} + \begin{bmatrix} 1 & & & & \\ & 1 & & & \\ & & 5 & & \\ & & & 5 & \\ & & & & 21 \end{bmatrix} \mathsf{X} + \begin{bmatrix} 1 & & & & \\ & 1 & & & \\ & & 5 & & \\ & & & 5 & \\ & & & & 5 \end{bmatrix} \mathsf{X}^2$$

$$+ \begin{bmatrix} 0 & & & & \\ & 0 & & & \\ & & 4 & & \\ & & & 4 & \\ & & & & 20 \end{bmatrix} \mathsf{X}^3.$$

calcula

$$\widehat{f}_4(M) = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 3 & 2 & 3 & 0 \\ 0 & 0 & 7 & 4 & 5 \\ 0 & 4 & 12 & 5 & 14 \\ 16 & 8 & 0 & 4 & 23 \end{bmatrix}.$$

Entonces, el usuario U_4 calcula los elementos K_7, K_8, K_9 y K_{10} como

$$K_7 = \widehat{f}_4(M)^{\widehat{r}_4} K_3 \widehat{f}_4(M)^{\widehat{s}_4} = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 \\ 2 & 0 & 2 & 3 & 2 \\ 4 & 4 & 7 & 5 & 5 \\ 8 & 8 & 8 & 5 & 13 \\ 0 & 24 & 8 & 8 & 23 \end{bmatrix},$$

$$K_8 = \widehat{f}_4(M)^{\widehat{r}_4} K_4 \widehat{f}_4(M)^{\widehat{s}_4} = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 2 & 0 & 0 \\ 0 & 6 & 1 & 2 & 4 \\ 8 & 12 & 2 & 8 & 10 \\ 0 & 16 & 12 & 10 & 5 \end{bmatrix},$$

$$K_9 = \widehat{f}_4(M)^{\widehat{r}_4} K_5 \widehat{f}_4(M)^{\widehat{s}_4} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 2 & 0 & 0 \\ 0 & 6 & 1 & 6 & 6 \\ 8 & 12 & 2 & 0 & 14 \\ 0 & 16 & 28 & 10 & 5 \end{bmatrix},$$

$$K_{10} = \widehat{f}_4(M)^{\widehat{r}_4} K_6 \widehat{f}_4(M)^{\widehat{s}_4} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 2 \\ 0 & 6 & 1 & 4 & 1 \\ 8 & 12 & 2 & 12 & 12 \\ 16 & 0 & 20 & 18 & 1 \end{bmatrix},$$

y éste le envía el vector $(K_6, K_7, K_8, K_9, K_{10})$ al nuevo usuario U_5.

Ahora, el usuario U_5 elige para su clave secreta $(r_5, s_5, f_5(M))$, donde $r_5 = 4$, $s_5 = 10$ y el polinomio $f_5(\mathsf{X})$ dado por la expresión

$$f_5(\mathsf{X}) = \begin{bmatrix} 0 & & & & \\ & 0 & & & \\ & & 0 & & \\ & & & 0 & \\ & & & & 16 \end{bmatrix} + \begin{bmatrix} 1 & & & & \\ & 1 & & & \\ & & 5 & & \\ & & & 13 & \\ & & & & 29 \end{bmatrix} \mathsf{X} + \begin{bmatrix} 0 & & & & \\ & 2 & & & \\ & & 6 & & \\ & & & 14 & \\ & & & & 30 \end{bmatrix} \mathsf{X}^2.$$

Entonces, calcula

$$f_5(M) = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 6 & 5 & 6 & 7 \\ 8 & 8 & 6 & 6 & 4 \\ 0 & 8 & 28 & 6 & 17 \end{bmatrix}$$

y, a continuación, el usuario U_5 calcula los elementos $L_1^{(5)}$, $L_2^{(5)}$, $L_3^{(5)}$, $L_4^{(5)}$ y $L_1^{(5)}$ como

$$L_1^{(5)} = f_5(M)^{r_5} K_6 f_5(M)^{s_5} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 2 & 0 & 0 \\ 0 & 2 & 3 & 2 & 6 \\ 8 & 4 & 6 & 0 & 2 \\ 0 & 16 & 20 & 14 & 23 \end{bmatrix},$$

$$L_2^{(5)} = f_5(M)^{r_5} K_7 f_5(M)^{s_5} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 2 \\ 0 & 6 & 1 & 0 & 3 \\ 8 & 12 & 2 & 4 & 0 \\ 16 & 0 & 4 & 18 & 17 \end{bmatrix},$$

$$L_3^{(5)} = f_5(M)^{r_5} K_8 f_5(M)^{s_5} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 2 & 0 & 0 \\ 0 & 6 & 1 & 6 & 6 \\ 8 & 12 & 2 & 0 & 14 \\ 0 & 16 & 28 & 10 & 21 \end{bmatrix},$$

$$L_4^{(5)} = f_5(M)^{r_5} K_9 f_5(M)^{s_5} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 2 & 0 & 0 \\ 0 & 6 & 1 & 2 & 0 \\ 8 & 12 & 2 & 8 & 2 \\ 0 & 16 & 12 & 10 & 21 \end{bmatrix},$$

$$L_5^{(5)} = f_5(M)^{r_5} K_{10} f_5(M)^{s_5} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 2 \\ 0 & 6 & 1 & 0 & 3 \\ 8 & 12 & 2 & 4 & 0 \\ 16 & 0 & 4 & 18 & 1 \end{bmatrix}.$$

El usuario U_5 considera que $S_5 = L_5^{(5)}$ es el nuevo secreto compatido por todos los miembros del sistema y, posteriormente, envía a cada uno de los usuarios el vector $\left(L_1^{(5)}, L_2^{(5)}, L_3^{(5)}, L_4^{(5)}\right)$.

Una vez recibido el vector anterior, el usuario U_1 toma la última componente, $L_4^{(5)}$ y calcula S_1 como

$$S_1 = f_1(M)^{r_1} L_4^{(5)} f_1(M)^{s_1} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 2 \\ 0 & 6 & 1 & 0 & 3 \\ 8 & 12 & 2 & 4 & 0 \\ 16 & 0 & 4 & 18 & 1 \end{bmatrix}.$$

Al mismo tiempo, el usuario U_2 toma la penúltima componente, $L_3^{(5)}$ y calcula el elemento S_2 como

$$S_2 = f_2(M)^{r_2} L_3^{(5)} f_2(M)^{s_2} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 2 \\ 0 & 6 & 1 & 0 & 3 \\ 8 & 12 & 2 & 4 & 0 \\ 16 & 0 & 4 & 18 & 1 \end{bmatrix}.$$

Por su parte, el usuario U_3, toma la componente $L_2^{(5)}$, para calcular el elemento S_3 como

$$S_3 = f_3(M)^{r_3} L_2^{(5)} f_3(M)^{s_3} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 2 \\ 0 & 6 & 1 & 0 & 3 \\ 8 & 12 & 2 & 4 & 0 \\ 16 & 0 & 4 & 18 & 1 \end{bmatrix}.$$

Por último, el usuario U_4, toma la primera de las componentes del vector recibido por el usuario U_5 y calcula S_4 como

$$S_4 = f_4(M)^{r_4} L_1^{(5)} f_4(M)^{s_4} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 2 \\ 0 & 6 & 1 & 0 & 3 \\ 8 & 12 & 2 & 4 & 0 \\ 16 & 0 & 4 & 18 & 1 \end{bmatrix}.$$

Observemos que todas estas últimas operaciones las realizan de forma simultánea e independiente por cada uno de los usuarios del sistema. Además, como consecuencia del teorema 4.5, tenemos que la clave secreta compartida es

$$S_1 = S_2 = S_3 = S_4 = S_5 = L_5^{(5)} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 2 \\ 0 & 6 & 1 & 0 & 3 \\ 8 & 12 & 2 & 4 & 0 \\ 16 & 0 & 4 & 18 & 1 \end{bmatrix}. \tag{4.32}$$

Supongamos ahora que el usuario U_2 abandona el sistema anterior que está compuesto por cinco usuarios. Entonces el usuario U_5 debe cambiar su clave privada, por ejemplo, $\left(\widehat{r}_5, \widehat{s}_5, \widehat{f}_5(\mathsf{X})\right)$, donde $\widehat{r}_5 = 7$, $\widehat{s}_5 = 3$ y el polinomio $\widehat{f}_5(\mathsf{X})$ viene dado por la expresión

$$\widehat{f}_5(\mathsf{X}) = \begin{bmatrix} 1 & & & & \\ & 3 & & & \\ & & 3 & & \\ & & & 11 & \\ & & & & 11 \end{bmatrix} + \begin{bmatrix} 1 & & & & \\ & 1 & & & \\ & & 1 & & \\ & & & 9 & \\ & & & & 9 \end{bmatrix} \mathsf{X} + \begin{bmatrix} 1 & & & & \\ & 1 & & & \\ & & 1 & & \\ & & & 1 & \\ & & & & 17 \end{bmatrix} \mathsf{X}^2$$
$$+ \begin{bmatrix} 0 & & & & \\ & 0 & & & \\ & & 4 & & \\ & & & 4 & \\ & & & & 4 \end{bmatrix} \mathsf{X}^3.$$

Ahora, calcula

$$\widehat{f}_5(M) = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 3 & 2 & 3 & 0 \\ 0 & 0 & 3 & 4 & 1 \\ 0 & 4 & 12 & 1 & 6 \\ 16 & 8 & 0 & 4 & 19 \end{bmatrix}.$$

Como el usuario U_5 tiene el vector $(K_6, K_7, K_8, K_9, K_{10})$, calcula los elementos $L_1^{(5)}$, $L_2^{(5)}$, $L_3^{(5)}$, $L_4^{(5)}$ y $L_5^{(5)}$ como

$$L_1^{(5)} = \widehat{f}_5(M)^{\widehat{r}_5} K_6 \widehat{f}_5(M)^{\widehat{s}_5} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 2 & 0 & 0 \\ 0 & 2 & 3 & 2 & 2 \\ 8 & 4 & 6 & 0 & 10 \\ 0 & 16 & 20 & 14 & 23 \end{bmatrix},$$

$$L_2^{(5)} = \widehat{f_5}(M)^{\widehat{r_5}} K_7 \widehat{f_5}(M)^{\widehat{s_5}} = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 \\ 2 & 0 & 0 & 2 & 3 \\ 4 & 0 & 3 & 7 & 1 \\ 0 & 0 & 8 & 1 & 7 \\ 16 & 0 & 24 & 16 & 19 \end{bmatrix},$$

$$L_3^{(5)} = \widehat{f_5}(M)^{\widehat{r_5}} K_8 \widehat{f_5}(M)^{\widehat{s_5}} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 2 & 0 & 0 \\ 0 & 6 & 1 & 6 & 2 \\ 8 & 12 & 2 & 0 & 6 \\ 0 & 16 & 28 & 10 & 21 \end{bmatrix},$$

$$L_4^{(5)} = \widehat{f_5}(M)^{\widehat{r_5}} K_9 \widehat{f_5}(M)^{\widehat{s_5}} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 2 & 0 & 0 \\ 0 & 6 & 1 & 2 & 4 \\ 8 & 12 & 2 & 8 & 10 \\ 0 & 16 & 12 & 10 & 21 \end{bmatrix},$$

$$L_5^{(5)} = \widehat{f_5}(M)^{\widehat{r_5}} K_{10} \widehat{f_5}(M)^{\widehat{s_5}} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 2 \\ 0 & 6 & 1 & 0 & 7 \\ 8 & 12 & 2 & 4 & 8 \\ 16 & 0 & 4 & 18 & 1 \end{bmatrix}.$$

Ahora, el usuario U_5 considera $S_5 = L_5^{(5)}$ y envía el vector $\left(L_1^{(5)}, L_2^{(5)}, L_3^{(5)}, L_4^{(5)}\right)$ a los usuarios que continúan en el sistema.

Nuevamente, el usuario U_1 utiliza la última componente $L_4^{(5)}$ del vector recibido del usuario U_5 y calcula S_1 como

$$S_1 = f_1(M)^{r_1} L_4^{(5)} f_1(M)^{s_1} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 2 \\ 0 & 6 & 1 & 0 & 7 \\ 8 & 12 & 2 & 4 & 8 \\ 16 & 0 & 4 & 18 & 1 \end{bmatrix}.$$

El usuario U_3 utiliza la segunda componente $L_2^{(5)}$ del vector recibido y calcula el elemento S_3 como

$$S_3 = f_3(M)^{r_3} L_2^{(5)} f_3(M)^{s_3} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 2 \\ 0 & 6 & 1 & 0 & 7 \\ 8 & 12 & 2 & 4 & 8 \\ 16 & 0 & 4 & 18 & 1 \end{bmatrix}.$$

Por último, el usuario U_4 utiliza la primera componente $L_1^{(5)}$ del vector recibido y calcula el elemento S_4 como

$$S_4 = f_4(M)^{r_4} L_1^{(5)} f_4(M)^{s_4} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 2 \\ 0 & 6 & 1 & 0 & 7 \\ 8 & 12 & 2 & 4 & 8 \\ 16 & 0 & 4 & 18 & 1 \end{bmatrix}.$$

Como consecuencia del teorema 4.5, ahora la clave secreta compartida es

$$S_1 = S_2 = S_3 = S_4 = S_5 = L_5^{(5)} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 2 \\ 0 & 6 & 1 & 0 & 7 \\ 8 & 12 & 2 & 4 & 8 \\ 16 & 0 & 4 & 18 & 1 \end{bmatrix}. \tag{4.33}$$

Notemos que la clave secreta en la operación unión de un miembro al sistema y en la operación de abandono de un miembro del sistema son diferentes, como se desprende al comparar las expresiones (4.32) y (4.33). Dicha diferencia se manifiesta en los elementos que ocupan las posiciones $(3, 5)$ y $(4, 5)$.

La gran similitud entre las claves se debe a que utilizamos un sistema con pocos usuarios, así como un primo p y un entero positivo m muy bajos. En aplicaciones prácticas reales, para evitar estas similitudes entre las claves secretas, es suficiente utilizar un primo de al menos tres cifras decimales, con el mismo entero m.

Capítulo 5

Conclusiones y líneas futuras de investigación

En esta memoria se proponen diversos protocolos de intercambio de claves y esquemas de multidifusión basados en el modelo de Diffie-Hellman sobre un anillo cualquiera R no conmutativo.

El análisis de la seguridad realizado concluye que la misma, está directamente relacionada con el número de elementos invertibles de los anillos sobre los que se estudian los protocolos. Más concretamente, es necesario que el número de elementos invertibles de R sea prácticamente nulo para garantizar la seguridad de los mismos.

Para el desarrollo de los protocolos de intercambio de claves y esquemas de multidifusión se han estudiado y caracterizado los anillos E_p y ${E_p}^{(m)}$, siendo ${E_p}^{(m)}$ una extensión de E_p. La utilización del anillo E_p presenta la ventaja de que podemos definir una aritmética sobre los elementos de E_p, que nos permite operar de forma eficiente desde el punto de vista computacional. Además, no es necesario utilizar primos grandes para alcanzar los niveles de seguridad que eviten los ataques conocidos hasta la fecha. Se ha puesto de manifiesto cómo con valores relativamente pequeños de los parámetros p y m se alcanza un nivel de seguridad equivalente al alcanzado por los protocolos clásicos definidos sobre cuerpos finitos, donde se utilizan primos de un gran tamaño y donde los requerimientos en recursos computacioneales son muy elevados.

Sin embargo, los anillos E_p y su extensión ${E_p}^{(m)}$ son únicamente un ejemplo de anillos no conmutativos sobre los que podemos considerar los protocolos y esquemas propuestos. Una de nuestras líneas futuras de investigación se plantea como objetivo

el desarrollo y estudio de estos protocolos sobre otros anillos no conmutativos, así como el diseño y estudio de nuevos protocolos sobre estos anillos. Otro aspecto que debe ser considerado sobre estos nuevos protocolos es el análisis exhaustivo de su seguridad.

Bibliografía

[1] L. Adleman. A subexponential algorithm for the discrete logarithm problem with applications to cryptography. En *Proceedings of the 20th Annual Symposium on Foundations of Computer Science*, páginas 13–27. The Graduate Center of the City University of New York (CUNY), New York, USA, 2003.

[2] R. Álvarez, L. Tortosa, J. Vicent y A. Zamora. A non-abelian group based on block upper triangular matrices with cryptographic applications. En M. Bras-Amorós y T. Høholdt (editores), *Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes*, volumen 5527 de *Lecture Notes in Computer Science*, páginas 117–126. Springer-Verlag, Berlin, 2009.

[3] R. Álvarez, L. Tortosa, J.-F. Vicent y A. Zamora. Analysis and design of a secure key exchange scheme. *Information Sciences*, **179**: 2014–2021 (2009).

[4] I. Anshel, M. Anshel, B. Fisher y D. Goldfeld. New key agreement protocols in braid group cryptography. En D. Naccache (editor), *Topics in Cryptology – CT-RSA 2001*, volumen 2020 de *Lecture Notes in Computer Science*, páginas 13–27. Springer-Verlag, Berlin, 2001.

[5] I. Anshel, M. Anshel y D. Goldfeld. An algebraic method for public-key cryptography. *Mathematical Research Letters*, **6**: 1–5 (1999).

[6] M. Anshel. Braid group cryptography and quantum crytoanalysis. En *8th International Wigner Annual Symposium on Foundations of Computer Science*, páginas 55–60. IEEE Computer Society Washington, Washington DC, USA, 2003.

[7] G. M. Bergman. Some examples in PI ring theory. *Israel Journal of Mathematics*, **18**: 257–277 (1974).

[8] D. J. Bernstein y A. K. Lenstra. A general number field sieve implementation. *Lecture Notes in Mathematics*, **1554**: 103–126 (1993).

[9] D. Boneh y R. J. Lipton. Quantum cryptanalysis of hidden linear functions. En D. Coppersmith (editor), *Advances in Cryptology – CRYPT0 '95*, volumen 963 de *Lecture Notes in Computer Science*, páginas 424–437. Springer-Verlag, Berlin, 1995.

[10] D. Boucher, P. Gaborit, W. Geiselmann, O. Ruatta y F. Ulmer. Key exchange and encryption schemes based on non-commutative skew polynomials. En N. Sendrier (editor), *Post-Quantum Cryptography*, volumen 6061 de *Lecture Notes in Computer Science*, páginas 126–141. Springer-Verlag, Berlin, 2010.

[11] J.-J. Climent, F. Ferrández, J.-F. Vicent y A. Zamora. A nonlinear elliptic curve cryptosystem based on matrices. *Applied Mathematics and Computation*, **174**: 150–164 (2006).

[12] J.-J. Climent, J. A. López-Ramos, P. R. Navarro y L. Tortosa. A key agreement protocol for distributed secure multicast on a non-commutative ring. En J. Vigo Aguiar (editor), *Proceedings of the 12th International Conference on Computational and Mathematical Methods in Science and Engineering (CMMSE 2012)*, páginas 329–335. 2012.

[13] J.-J. Climent, J. A. López-Ramos, P. R. Navarro y L. Tortosa. Key agreement protocols for distributed secure multicast over the ring $E_p{}^{(m)}$. *WIT Transactions on Information and Communication Technologies*, **45**: 13–24 (2013).

[14] J.-J. Climent, P. R. Navarro y L. Tortosa. Key exchange protocols over noncommutative rings. The case $\mathrm{End}(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$. En J. Vigo Aguiar (editor), *Proceedings of the 11th International Conference on Computational and Mathematical Methods in Science and Engineering (CMMSE 2011)*, páginas 357–364. 2011.

[15] J.-J. Climent, P. R. Navarro y L. Tortosa. On the arithmetic of the endomorphisms ring $\mathrm{End}(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$. *Applicable Algebra in Engineering, Communication and Computing*, **22(2)**: 91–108 (2011).

[16] J.-J. Climent, P. R. Navarro y L. Tortosa. Key exchange protocols over noncommutative rings. The case of $\mathrm{End}(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$. *International Journal of Computer Mathematics*, **89(13–14)**: 1753–1763 (2012).

[17] J.-J. Climent, P. R. Navarro y L. Tortosa. An extension of the noncommutative Bergman's ring with a large number of noninvertible elements.

Submitted, (2013).

[18] D. Coppersmith. Weakness in quaternion signatures. *Journal of Cryptology*, **14(2)**: 77–85 (2001).

[19] M. Cotton, L. Vegoda, ICANN y D. Meyer. IANA guidelines for IPv4 multicast address assignements. Internet Engineering Task Force (IETF), RFC5771, 2010. http://tools.ietf.org/html/rfc5771.

[20] A. Cunningham. *Haupt-exponents, residue-indices, primitive roots, and standard congruences*. Francis Hodgson, London, 1922.

[21] S. E. Deering. Multicast routing in internetworks and extended LANs. En *Proceedings of the Symposium on Communications Architectures and Protocols (SIGCOMM '88)*, páginas 15–64. Stanford, CA, 1988.

[22] W. D. Diffie y M. E. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, **22(6)**: 644–654 (1976).

[23] V. Dubois y J.-G. Kammerer. Cryptanalysis of cryptosystems based on non-commutative skew polynomials. En D. Catalano, N. Fazio, R. Gennaro y A. Nicolosi (editores), *Public Key Cryptography – PKC 2011*, volumen 6571 de *Lecture Notes in Computer Science*, páginas 459–472. Springer-Verlag, Berlin, 2011.

[24] T. ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transactions on Information Theory*, **31(4)**: 469–472 (1985).

[25] R. W. Floyd. Nondeterministic algorithms. *Journal of the ACM*, **14(4)**: 636–644 (1967).

[26] C. Gentry. Key recovery and message attacks on NTRU-composite. En B. Pfitzmann (editor), *Advances in Cryptology – EUROCRYPT 2001*, volumen 2045 de *Lecture Notes in Computer Science*, páginas 182–194. Springer-Verlag, Berlin, 2001.

[27] C. Gentry y M. Szydlo. Cryptanalysis of the revised NTRU signature scheme. En L. Knudsen (editor), *Advances in Cryptology – EUROCRYPT 2002*, volumen 2332 de *Lecture Notes in Computer Science*, páginas 299–320. Springer-Verlag, Berlin, 2002.

[28] J. Hoffstein, J. Pipher y J. H. Silverman. NTRU: a ring-based public key cryptosystem. En J. P. Buhler (editor), *Algorithmic Number Theory*, volumen 1423 de *Lecture Notes in Computer Science*, páginas 267–288. Springer-Verlag,

Berlin, 1998.

[29] B. Hurley y T. Hurley. Group ring cryptography. *International Journal of Pure and Applied Mathematics*, **60(1)**: 67–86 (2011).

[30] A. A. Kamal y A. M. Youssef. Cryptanalysis of a key exchange protocol based on the endomorphisms ring End($\mathbb{Z}_p \times \mathbb{Z}_p^2$). *Applicable Algebra in Engineering, Communication and Computing*, **23(3–4)**: 143–149 (2012).

[31] K. H. Ko, J. W. Lee y T. Thomas. Towards generating secure keys for braid cryptography. *Designs, Codes and Cryptography*, **45(3)**: 317–333 (2007).

[32] K. H. Ko, S. J. Lee, J. H. Cheon, J. W. Han, J.-s. Kang y C. Park. New public-key cryptosystem using braid groups. En M. Bellare (editor), *Advances in Cryptology – CRYPTO 2000*, volumen 1880 de *Lecture Notes in Computer Science*, páginas 166–183. Springer-Verlag, Berlin, 2000.

[33] M. Kraitchik. *Théorie des nombres*. Gauthier-Villars, Paris, France, 1922.

[34] M. Kraitchik. *Recherches sur la théorie des nombres*. Gauthier-Villars, Paris, France, 1924.

[35] T.-Y. Lam. *A First Curs in Noncommutative Rings*. Número 131 en Graduate Texts in Mathematics. Springer, New York, NY, segunda edición, 2001.

[36] H. W. Lenstra, Jr. Factoring integers with elliptic curves. *Annals of Mathematics*, **126**: 649–673 (1987).

[37] A. J. Menezes, P. C. van Oorschot y S. A. Vanstone. *Handbook of Applied Cryptography*. CRC Press, Boca Raton, FL, 1996.

[38] A. J. Menezes y Y.-H. Wu. The discrete logarithm problem in $GL(n, q)$. *Ars Combinatoria*, **47**: 23–32 (1997).

[39] A. G. Myasnikov, V. Shpilrain y A. Ushakov. *Group-based cryptography*. Birkhäuser Verlag, Basel, Switzerland, 2008.

[40] R. W. K. Odoni, V. Varadharajan y P. W. Sanders. Public key distribution in matrix rings. *Electronics Letters*, **20**: 386–387 (1984).

[41] S.-H. Paeng, K.-C. Ha, J. H. Kim, S. Chee y C. Park. New public key cryptosystem using finite non abelian groups. En J. Kilian (editor), *Advances in Cryptology – CRYPTO 2001*, volumen 2139 de *Lecture Notes in Computer Science*, páginas 470–485. Springer-Verlag, Berlin, 2001.

[42] J. M. Pollard. Monte carlo methods for index computation mod$p$. *Mathematics of Computation, American Mathematical Society*, **32**: 918–924 (1978).

[43] J. Pollard. A monte carlo method for factorization. *BIT Numerical Mathe-*

matics, **15(3)**: 331–334 (1975).

[44] C. Pomerance. Analysis and comparison of some integer factoring algorithms. *Computational Methods in Number Theory*, **I**: 89–139 (1982).

[45] S. Rafaeli y D. Hutchison. A survey of key management for secure group communication. *ACM Computing Surveys*, **35(3)**: 309–329 (2003).

[46] R. L. Rivest, A. Shamir y L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, **21(2)**: 120–126 (1978).

[47] E. Sakalauskas y T. Burba. Basic semigroup primitive for cryptographic session key exchange protocol (SKEP). *Information Technology and Control*, **28(3)**: 76–80 (2003).

[48] T. Satoh y K. Araki. On construction of signature scheme over a certain non-commutative ring. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, **E80-A(1)**: 40–45 (1997).

[49] B. Schneier. *Applied Cryptography*. John Wiley & Sons, New York, NY, segunda edición, 1996.

[50] P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, **26(5)**: 1484–1509 (1997).

[51] V. Shpilrain. Cryptanalysis of Stickel's key exchange scheme. En E. A. Hirsch, A. A. Razborov, A. Semenov y A. Slissenko (editores), *Computer Science – Theory and Applications*, volumen 5010 de *Lecture Notes in Computer Science*, páginas 283–288. Springer-Verlag, Berlin, 2008.

[52] V. Shpilrain y A. Ushakov. A new key exchange protocol based on the decomposition problem. *Contemporary Mathematics*, **418**: 161–167 (2006).

[53] V. M. Sidelnikov, M. A. Cherepnev y V. V. Yashchenko. Systems of open distribution of keys on the basis of noncommutative semigroups. *Russian Academy of Sciences. Doklady Mathematics*, **48(2)**: 384–386 (1994).

[54] M. Steiner, G. Tsudik y M. Waidner. Diffie-Hellman key distribution extended to group communication. En *Proceedings of the 3rd ACM Conference on Computer and Communications Security*, páginas 31–37. ACM, New York, NY, 1996.

[55] M. Steiner, G. Tsudik y M. Waidner. Key agreement in dynamic peer groups. *IEEE Transactions of Parallel and Distributed Systems*, **11(8)**: 769–

780 (2000).

[56] E. Stickel. A new method for exchanging secret keys. En *Proceedings of the Third International Conference on Information Technology and Applications (ICITA'05)*, páginas 426–430. Sidney, Australia, 2005.

[57] D. R. Stinson. *Cryptography. Theory and Practice*. CRC Press, Boca Raton, FL, 1995.

[58] T. Thomas y A. K. Lal. A zero-knowledge undeniable signature scheme in non-abelian group setting. *International Journal of Network Security*, **6(3)**: 265–269 (2008).

[59] V. Varadharajan y R. W. K. Odoni. Security of public key distribution in matrix rings. *Electronics Letters*, **22**: 46–47 (1986).

[60] A. E. Western y J. C. P. Miller. *Royal Society Mathematical Tables: Volume 9, Indices and Primitive Roots*. Cambridge University Press, Cambridge, UK, 1968.

[61] H. Yoo, S. Hong, S. Lee, J. Lim, O. Yi y M. Sung. A proposal of a new public key cryptosystem using matrices over a ring. En E. Dawson, A. Clark y C. Boyd (editores), *Information Security and Privacy*, volumen 1841 de *Lecture Notes in Computer Science*, páginas 41–48. Springer-Verlag, Berlin, 2000.

[62] S. Zhu y S. Jajodia. Scalable group key management for secure multicast: A taxonomy and new directions. En S. C.-H. Huang, D. MacCallum y D.-Z. Du (editores), *Network Security*, páginas 57–75. Springer, New York, 2010.