Criptosistemas de clave pública basados en acciones del anillo $E_p^{(m)}$

Joan-Josep Climent
Departament d'Estadística
i Investigació Operativa
Universitat d'Alacant
Email: jcliment@ua.es

Juan A. López-Ramos
Departamento de Matemáticas
Universidad de Almería
Email: jlopez@ual.es

Leandro Tortosa
Departament de Ciència de la
Computació i Intel·igència Artificial
Universitat d'Alacant
Email: tortosa@ua.es

***Abstract*—El objetivo de este trabajo es la introducción de aplicaciones criptográficas de una extensión del anillo $\mathrm{End}(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$, denotado por $E_p^{(m)}$. Mostramos cómo las acciones del anillo $E_p^{(m)}$ sobre dos conjuntos distintos nos permiten introducir dos criptosistemas de clave pública diferentes y basados en la dificultad de resolver los problemas de la acción del semigrupo y de la descomposición respectivamente. Observamos cómo la no conmutatividad del anillo, así como la existencia de un gran número de divisores de cero lo hacen apropiado para tales aplicaciones criptográficas.**

***Palabras clave*—Criptosistema de Clave Pública (*Public Key Cryptosystem*), Problema de la Descomposición (*Decomposition Problem*), Problema de la Acción del Semigrupo (*Semigroup Action Problem*).**

I. Nomenclatura

SAP, Problema de la Acción del Semigrupo (Semigroup Action Problem).

DP, Problema de la Descomposición (Decomposition Problem).

$\mathrm{Mat}_{m\times m}(\mathbb{Z})$, matrices cuadradas de tamaño $m \times m$ sobre el anillo de los número enteros.

$r = (r_0, r_1, \ldots, r_{m-1})$, denota una matriz columna de m componentes.

E_p, anillo de matrices de tamaño 2×2 isomorfo al anillo $\mathrm{End}(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$.

$E_p^{(m)}$, anillo de matrices de tamaño $m \times m$ y que es extensión del anillo E_p.

II. Introducción

Desde que en [4] Diffie y Hellman proponen el primer protocolo de intercambio de claves a través de un canal público, son muchos los autores que han introducido esquemas de este tipo, como por ejemplo [11], [12], [14], [16]. Si nos centramos en los criptosistemas de clave pública, podemos destacar indudablemente como los más conocidos [5] y [13]. Todos estos algoritmos, al igual que la idea original de Diffie y Hellman basan su fortaleza en la resolución de problemas sobre Teoría de Números. Por otro lado, trabajos como [15] o [9] en los que se muestran debilidades de [4], [5] y [13] y [12] respectivamente, así como los constantes avances en computación y capacidad de cálculo de las máquinas actuales han llevado a considerar otras estructuras para el desarrollo de tales protocolos de intercambio de clave y de criptosistemas de clave pública, tales como el conjunto de puntos de una curva elíptica ([7] y [10]) o cómo la acción de un semigrupo sobre un conjunto puede dar lugar también a este tipo de algoritmos [8]. En este caso, los autores muestran cómo es posible definir un criptosistema similar al de ElGamal [5] aprovechando la acción del semigrupo sobre un conjunto. Sin embargo, en este caso, un atacante debe resolver el conocido como *Problema de la Acción del Semigrupo* o SAP (*Semigroup Action Problem*), que consiste en dado un grupo abeliano finito G, un conjunto finito S y una acción de G sobre S, si dados $x, y \in S$ tales que $y = g \cdot x$ para algún $g \in G$, encontrar $h \in G$ tal que $y = h \cdot x$.

Basándose en el protocolo de intercambio de clave introducido en [16], Climent *et al.* en [2] introducen un protocolo de intercambio de clave para dos comunicantes sobre el anillo $\mathrm{End}(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$. Sin embargo, aprovechando los elementos invertibles de anillo, Kamal y Youssef en [6] llevan a cabo un ataque a dicho protocolo de intercambio de claves. De este modo, y buscando evitar este tipo de ataques, en [1] los autores introducen un esquema general de intercambio de claves para un conjunto finito de usuarios, que extiende el de [2], pero que además se lleva a cabo sobre una extensión del anillo anterior, el anillo $E_p^{(m)}$, estudiado en [3], y en el que los elementos invertibles son muy escasos. La fortaleza de este nuevo intercambio de claves extiende el intercambio de clave de Diffie-Hellman, pero se basa en un problema mucho más duro que el del logaritmo discreto y que es conocido como *Problema de la Descomposición* o DP (*Decomposition Problem*), es decir, dado un grupo G, un subconjunto $S \subseteq G$ y un elemento $(x, y) \in G \times G$, encontrar elementos $z_1, z_2 \in S$ tales que $y = z_1 x z_2$.

El objetivo de este trabajo es usar la acción del semigrupo multiplicativo $E_p^{(m)}$ sobre un par de conjuntos para definir criptosistemas de clave pública en un entorno no conmutativo y basados en problemas distintos a los clásicos de Teoría de Números y de mucha más difícil resolución. En la sección III introducimos brevemente el anillo $E_p^{(m)}$, ampliamente estudiado en [3]. A continuación, en la sección IV y dado que los elementos de $E_p^{(m)}$ se expresan como matrices, usamos la acción de $E_p^{(m)}$ sobre una columna de elementos de un elemento en $E_p^{(m)}$ para definir un criptosistema basado en el

ISBN: 978-84-9717-323-0

problema SAP. En la sección V, es la acción del propio anillo $E_p^{(m)}$ sobre sí mismo la que se usa para definir un criptosistema basado en el problema DP. La sección VI concluye los resultados introducidos en este trabajo.

III. El anillo $E_p^{(m)}$

En [2] los autores prueban que el anillo $\mathrm{End}(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$ es isomorfo a un anillo que los autores denotan por E_p y cuyos elementos pueden representarse como matrices del tipo

$$\begin{bmatrix} a & b \\ pc & d \end{bmatrix} \quad \text{con } a, b, c \in \mathbb{Z}_p \text{ y } d \in \mathbb{Z}_{p^2}.$$

Motivados por los resultados citados en la introducción sobre el criptoanálisis llevado acabo sobre el anillo anterior, Climent *et al.* introducen en [3] la siguiente extensión del anillo E_p. Dado un primo p y un entero m, se define el conjunto

$$E_p^{(m)} = \Big\{ [a_{ij}] \in \mathrm{Mat}_{m\times m}(\mathbb{Z}) \mid a_{ij} \in \mathbb{Z}_{p^i} \text{ si } i \le j \text{ y } a_{ij} \in p^{i-j}\mathbb{Z}_{p^i} \text{ si } i > j \Big\}.$$

Asimismo se pueden definir una adición y una multiplicación como

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

Se prueba entonces el siguiente resultado.

Teorema 1: *El conjunto $E_p^{(m)}$ con la adición y la multiplicación definidas anteriormente es un anillo no conmutativo.*

También en [3] se prueban las siguientes propiedades del anillo $E_p^{(m)}$ y que a continuación se relacionan.

Teorema 2: *El centro del anillo $E_p^{(m)}$ es el conjunto dado por*

$$Z(E_p^{(m)}) = \Big\{ [a_{ij}] \in E_p^{(m)} \mid a_{ij} = 0 \text{ si } i \neq j \text{ y } a_{ii} = \sum_{r=1}^{i} p^{i-r} u_{i-r} \text{ con } u_{i-r} \in \mathbb{Z}_p \Big\}.$$

Teorema 3: *Un elemento $[a_{ij}] \in E_p^{(m)}$ es invertible si y sólo si $a_{ii} \not\equiv_p 0$ para $i = 1, 2, \ldots, m$.*

Teorema 4: *El cardinal de $E_p^{(m)}$ es p^{ν_m} donde $\nu_m = (2m^3 + 3m^2 + m)/6$ y el cardinal del conjunto de los elementos invertibles viene dado por $p^{\nu_m - m}(p-1)^m$.*

Observación 1: A partir de los resultados anteriores y a modo de ejemplo, puede comprobarse que en $E_2^{(32)}$, el porcentaje de elementos no invertibles alcanza el 99.9999999767%.

IV. Un criptosistema de clave pública sobre $E_p^{(m)}$ basado en el SAP

El propósito de esta sección es la introducción de un criptosistema de clave pública basado en la acción del semigrupo multiplicativo de $E_p^{(m)}$ sobre el conjunto $\mathbb{Z}_p \times \mathbb{Z}_{p^2} \times \cdots \times \mathbb{Z}_{p^m}$. Dicha acción viene dada por la multiplicación definida sobre el anillo $E_p^{(m)}$, es decir, la acción que tiene lugar al multiplicar las filas del primer elemento por cada una de las columnas del segundo. Consideremos pues el anillo de polinomios $Z(E_p^{(m)})[X]$ con coeficientes sobre el centro del anillo $E_p^{(m)}$.

Algoritmo 1: *Sea $M \in E_p^{(m)}$ un valor público y $s \in \mathbb{Z}_p \times \mathbb{Z}_{p^2} \times \cdots \times \mathbb{Z}_{p^m}$ el mensaje que el comunicante Bernardo quiere enviar a Alberto de forma confidencial. Entonces:*

- *Alberto escoge $r \in \mathbb{Z}_p \times \mathbb{Z}_{p^2} \times \cdots \times \mathbb{Z}_{p^m}$, $f(X) \in Z(E_p^{(m)})[X]$ y calcula $t = f(M) \cdot r$.*
- *Alberto publica el par (r, t), manteniendo en secreto su propia clave privada $f(M)$.*
- *Bernardo elige $g(X) \in Z(E_p^{(m)})[X]$ y envía a Alberto el par*
$$(c_1, c_2) = (g(M) \cdot r, s + g(M) \cdot t).$$
- *Alberto obtiene $s = c_2 - f(M) \cdot c_1$.*

Notemos que aunque $E_p^{(m)}$ no es conmutativo, se tiene que $f(M)g(M) = g(M)f(M)$. De este modo se tiene el siguiente resultado.

Teorema 5: *El algoritmo 1 es correcto.*

Podemos observar que romper el algoritmo anterior involucra resolver el problema SAP, es decir, conocidos los valores r y $t = f(M) \cdot r \in \mathbb{Z}_p \times \mathbb{Z}_{p^2} \times \cdots \times \mathbb{Z}_{p^m}$, encontrar un elemento $A \in E_p^{(m)}$ que verifique $t = A \cdot r$. En [8] los autores prueban que cuanto más cerca se halle el semigrupo que actúa sobre el conjunto correspondiente de ser un grupo, es decir, cuanto más grande sea el conjunto de elementos invertibles en dicho semigrupo, más fácil es utilizar una versión sobre dicho semigupo del algoritmo del Polling-Hellman para el cálculo del logaritmo discreto. En nuestro caso, tal y como se ha indicado anteriormente, el número de elementos no invertibles puede acercarse mucho al total de elementos de $E_p^{(m)}$ con una adecuada elección de p y m.

Una característica adicional del criptosistema anterior es el uso de un polinomio distinto $g(X)$ cada vez que se cifra un mensaje. En el criptosistema de ElGamal, [5], la elección de un parámetro aleatorio para cada cifrado es necesaria para evitar un ataque texto claro-texto cifrado basado en la existencia de inversos. Sin embargo, en este caso, un ataque tal no podría llevarse a cabo debido a la ya citada escasa existencia de inversos. De hecho no puede llevarse a cabo ningún ataque basado en la división por no tratarse $E_p^{(m)}$ de un dominio de integridad. Además, la elección de dicho polinomio $g(X)$ de forma aleatoria evita ataques por repetición, pues un mismo mensaje no es cifrado dos veces del mismo modo.

Dada la clave pública (r, t), con $t = f(M) \cdot r$, sea A una solución del SAP, es decir, $A \cdot r = t$ y supongamos que el

elemento $g(M)$ verifica que $Ag(M) = g(M)A$. Entonces, dado el mensaje cifrado

$$(c_1, c_2) = (g(M) \cdot r, s + g(M) \cdot t)$$

tenemos que

$$\begin{aligned} & s + g(M) \cdot t - Ag(M) \cdot r \\ & = s + g(M)f(M) \cdot r - g(M)A \cdot r \\ & = s + g(M)f(M) \cdot r - g(M)f(M) \cdot r = s. \end{aligned}$$

De este modo es vital que el elemento $g(M)$ no conmute con la solución encontrada del SAP, A. Veamos que podemos tener condiciones para que ni $g(M)$ ni A sean elementos del centro de $E_p^{(m)}$.

La demostración del siguiente resultado es inmediata.

Lema 1: *Sea R un anillo no conmutativo. Entonces $Z(R[X]) = Z(R)[X]$.*

Una consecuencia directa del lema anterior nos da que $Z(E_p^{(m)}[X]) = Z(E_p^{(m)})[X]$.

Veamos ahora una condición para que $g(M)$ no sea un elemento central en $E_p^{(m)}$.

Lema 2: *Sea $g(X) = g_0 + g_1X + \cdots + g_kX^k \in Z(E_p^{(m)}[X])$ tal que $(g_j)_{i,i} \not\equiv_p 0$ para todo $i = 1, 2, \ldots, m$ y para algún $j = 1, 2, \ldots, k$. Si $M \notin Z(E_p^{(m)})$, entonces $g(M) \notin Z(E_p^{(m)})$.*

Demostración 1 (Demostración): Como $(g_j)_{i,i} \not\equiv_p 0$ para todo $i = 1, 2, \ldots, m$, tenemos que g_j es invertible. De este modo, si N es cualquier elemento en $E_p^{(m)}$ y suponemos que $Ng_jM = g_jMN$, entonces $g_jNM = g_jMN$, con lo que $MN = NM$, lo que es una contradicción. De este modo, aunque g_iM^i sea un elemento central para cualquier $i = 0, 1, 2, \ldots, k$ con $i \neq j$, tenemos que $g(M) \notin Z(E_p^{(m)})$.

Supongamos ahora que un atacante intenta encontrar A central y que sea solución del SAP $A \cdot r = t$. En tal caso, el elemento A ha de tener la forma

$$\operatorname{diag}(a_0, a_0 + pa_1, \ldots, a_0 + pa_1 + \cdots + p^{m-1}a_{m-1}),$$

con $a_i \in \mathbb{Z}_p$ para todo $i = 0, 1, 2, \ldots, m-1$.

Teorema 6: *Supongamos que*

$$\operatorname{diag}(a_0, a_0 + pa_1, \ldots, a_0 + pa_1 + \cdots + p^{m-1}a_{m-1}),$$

y que $r = (r_0, r_1, \ldots, r_{m-1})$ y $t = (t_0, t_1, \ldots, t_{m-1})$ son elementos de $\mathbb{Z}_p \times \mathbb{Z}_{p^2} \times \cdots \times \mathbb{Z}_{p^m}$ tales que $A \cdot r = t$. Si $r_i \not\equiv_p 0$ para $i = 0, 1, 2, \ldots, m-1$ entonces

$$r_0^{-1}t_0 \equiv_p r_1^{-1}t_1 \equiv_p \cdots \equiv_p r_{m-1}^{-1}t_{m-1}.$$

Demostración 2 (Demostración): De la igualdad $A \cdot r = t$ tenemos las siguientes igualdades

$$\begin{aligned} a_0r_0 &\equiv_p t_0, \\ (a_0 + pa_1)r_1 &\equiv_{p^2} t_1, \\ &\cdots \\ (a_0 + pa_1 + \cdots + p^{m-1}a_{m-1})r_{m-1} &\equiv_{p^m} t_{m-1}. \end{aligned}$$

Entonces $a_0 \equiv_p r_0^{-1}t_0$. De este modo $a_0 = r_0^{-1}t_0 + hp$ con $h \in \mathbb{Z}$. De la segunda expresión tenemos que $pa_1r_1 \equiv_{p^2} t_1 - a_0r_1$ y de este modo, $\operatorname{mcd}(pr_1, p^2) = p \mid (t_1 - a_0r_1)$. Por tanto, $t_1 \equiv_p a_0r_1$ y así $r_0^{-1}t_0 \equiv_p r_1^{-1}t_1$.

Supongamos ahora que

$$r_0^{-1}t_0 \equiv_p r_1^{-1}t_1 \equiv_p \cdots \equiv_p r_{m-2}^{-1}t_{m-2}.$$

De la expresión

$$a_0 + pa_1 + \cdots + p^{m-2}a_{m-2} \equiv_{p^{m-1}} r_{m-2}^{-1}t_{m-2},$$

tenemos que $a_0 + pa_1 + \cdots + p^{m-2}a_{m-2} = r_{m-2}^{-1}t_{m-2} + p^{m-1}h$ para algún $h \in \mathbb{Z}$. Entonces, como

$$(a_0 + pa_1 + \cdots + p^{m-1}a_{m-1})r_{m-1} \equiv_{p^m} t_{m-1}$$

tenemos que

$$a_0 + pa_1 + \cdots + p^{m-2}a_{m-2} + p^{m-1}a_{m-1} \equiv_{p^m} r_{m-1}^{-1}t_{m-1}$$

y por tanto $r_{m-2}^{-1}t_{m-2} + p^{m-1}(h + a_{m-1}) \equiv_{p^m} r_{m-1}^{-1}t_{m-1}$, de donde $r_{m-2}^{-1}t_{m-2} \equiv_p r_{m-1}^{-1}t_{m-1}$.

La consecuencia del resultado anterior es que dado el elemento $f(M)$, un usuario puede tomar como clave pública el par (r, t) con $r = (r_0, r_1, \ldots, r_{m-1})$ y $t = (t_0, t_1, \ldots, t_{m-1})$ con $r_i, t_i \in \mathbb{Z}_{p^{i+1}}$, para $i = 0, 1, 2, \ldots, m-1$ tales que $f(M) \cdot r = t$ y con r_k no divisible por p para ningún $k = 0, 1, 2, \ldots, m-1$ y de modo que exista i tal que $r_i^{-1}t_i \not\equiv_p r_0^{-1}t_0$, haciendo imposible que un atacante pueda calcular un elemento central A solución del SAP anterior.

Un ataque por fuerza bruta supondría probar con todos los posibles polinomios con coeficientes en el centro de $E_p^{(m)}$. Si consideramos un primo con 20 cifras decimales, o lo que es lo mismo, aproximadamente de 64 bits, y el entero $m = 5$, tenemos que el número de polinomios es del orden de 10^{121}. La longitud de los mensajes cifrados en este caso sería

$$2 \cdot (1024 + 512 + 256 + 128 + 64) = 9920 \text{ bits}.$$

V. Un criptosistema de clave pública sobre $E_p^{(m)}$ basado en el DP

La acción del semigrupo multiplicativo de $E_p^{(m)}$ sobre el propio conjunto $E_p^{(m)}$ nos define un criptosistema similar basado también en el SAP. Sin embargo, nuestro objetivo ahora es el de introducir un criptosistema de clave pública basado en los intercambios de clave introducidos en [1]. Consideramos la acción arriba indicada, aunque presentamos la siguiente variación. El algoritmo que introducimos, utilizando la misma notación que en el algoritmo 1, es como sigue:

Algoritmo 2: *Sea $M \in E_p^{(m)}$ un valor público y $S \in E_p^{(m)}$ el mensaje que el comunicante Bernardo quiere enviar a Alberto de forma confidencial. Entonces:*

- *Alberto escoge $N \in E_p^{(m)}$ tal que $MN \neq NM$, $f(X) \in Z(E_p^{(m)})[X]$ y un par de enteros positivos (u, v) y calcula $f(M)^uNf(M)^v$.*
- *Alberto publica el par $(N, f(M)^uNf(M)^v)$, manteniendo en secreto su propia clave privada $f(M)$ junto con los enteros u y v.*

- *Bernardo elige $g(X) \in Z(E_p^{(m)})[X]$ y un par de enteros positivos (r,t) y envía a Alberto el par*

$$(c_1,c_2) = \Big(g(M)^r N g(M)^t, \\ S + g(M)^r f(M)^u N f(M)^v g(M)^t\Big).$$

- *Alberto obtiene $S = c_2 - f(M)^u c_1 f(M)^v$.*

De nuevo, como en la sección anterior, el hecho de que $f(X)$ y $g(X)$ sean elementos del centro de $E_p^{(m)}[X]$ nos proporciona el siguiente resultado.

Teorema 7: *El algoritmo 2 es correcto.*

Teorema 8: *Romper el criptosistema dado por el algoritmo 2 es equivalente a resolver el problema DP.*

Demostración 3 (Demostración): Supongamos en primer lugar que somos capaces de resolver el problema DP dado por el par $(N, f(M)^u N f(M)^v)$. Entonces somos capaces de encontrar Z_1 y Z_2 tales que $g(M)^u N g(M)^v = Z_1 N Z_2$, $Z_1 M = M Z_1$ y $Z_2 M = M Z_2$. Entonces

$$\begin{aligned} c_2 - Z_1 c_1 Z_2 &= S + g(M)^r f(M)^u N f(M)^v g(M)^t \\ &\quad - Z_1 g(M)^r N g(M)^t Z_2 \\ &= S + g(M)^r f(M)^u N f(M)^v g(M)^t \\ &\quad - g(M)^r Z_1 N Z_2 g(M)^t \\ &= S + g(M)^r f(M)^u N f(M)^v g(M)^t \\ &\quad - f(M)^u g(M)^r N g(M)^t f(M)^v \\ &= S. \end{aligned}$$

Por otro lado, sean A y B elementos de $E_p^{(m)}$. Ciframos entonces el elemento B usando la clave pública $(A, f(M)^u A f(M)^v)$. El cifrado es entonces

$$(c_1,c_2) = \Big(g(M)^r A g(M)^t, \\ B + g(M)^r f(M)^u A f(M)^v g(M)^t\Big)$$

para $g(X)$, r y t como en el algoritmo 2.

Si recíprocamente estamos suponiendo que somos capaces de descifrar el mensaje anterior obteniendo B sin conocer la clave privada, entonces podemos calcular el elemento $c_2 - B$, lo que es equivalente a conocer la clave compartida por los comunicantes $g(M)^r f(M)^u A f(M)^v g(M)^t$, que es equivalente a resolver los problemas DP dados por los pares

$$(A, g(M)^r A g(M)^t) \quad \text{y} \quad (A, f(M)^u A f(M)^v).$$

Veamos ahora que el ataque introducido en [6] para romper el intercambio de claves dado en [2] no es posible en el caso del algoritmo 2, dependiendo de los parámetros escogidos. El ataque se basa en encontrar elementos W_1, W_2 de $E_p^{(m)}$ tales que

$$W_1 M = M W_1, \quad W_2 M = M W_2, \\ g(M)^r N g(M)^t W_2 = W_1 N.$$

Entonces tenemos que

$$\begin{aligned} W_1 f(M)^u N f(M)^v W_2^{-1} &= f(M)^u W_1 N W_2^{-1} f(M)^v \\ &= f(M)^u g(M)^r N g(M)^t f(M)^v \end{aligned}$$

puesto que $W_i f(M)^k = f(M)^k W_i$ para $i = 1, 2$ y cualquier valor de k. Por tanto, podemos calcular

$$c_2 - W_1 f(M)^u N f(M)^v W_2^{-1} = S.$$

Sin embargo, la existencia de W_2^{-1} en $E_p^{(m)}$ es casi improbable dependiendo de los valores de p y m tal y como ya se deja patente en la la observación 1.

VI. Conclusión

En este trabajo hemos mostrado cómo la acción de un semigrupo multicativo y no conmutativo puede ser usada para la definición de criptosistemas de clave pública cuya fortaleza reside en la resolución de problemas computacionalmente difíciles. En un caso obtenemos un criptosistema cuya seguridad se basa en el problema de la descomposición proveniente de la acción que define la multiplicación de elementos en el anillo no conmutativo $E_p^{(m)}$. Dado que los elementos de dicho anillo pueden representarse como matrices, si restringimos esta acción a las columnas de las mismas, obtenemos entonces un nuevo criptosistema basado esta vez en el problema de la acción del semigrupo. En ambos casos mostramos cómo las propias características del anillo en lo que se refiere a la no conmutatividad y a la gran existencia de elementos divisores de cero evitan diferentes posibles criptoanálisis.

Agradecimientos

El primer autor ha sido parcialmente financiado por el proyecto MTM2011-24858 del Ministerio de Economía y Competitividad del Gobierno de España. El segundo autor está financiado por el grupo de investigación de la Junta de Andalucía FQM 211.

Referencias

[1] J.-J. Climent, J.A. López-Ramos, P.R. Navarro, L. Tortosa, "Key agreement protocols for distributed secure multicast over the ring $E_p^{(m)}$," *WIT Transactions on Information and Communication Technologies*, vol. 45, pp. 13–24, 2013.

[2] J.-J. Climent, P.R. Navarro, 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*, vol. 89(13-14), pp. 1753–1763, 2012.

[3] J.-J. Climent, P.R. Navarro, L. Tortosa, "An extension of the noncommutative Bergman's ring with a large number of noninvertible elements," enviado para su publicación.

[4] W.D. Diffie, M.E. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. 22(6), pp. 644–654, 1976.

[5] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Transactions Information Theory*, vol. 31(4), pp. 469–472, 1985.

[6] A.A. Kamal, A.M. Youssef, "Cryptanalysis of a key exchange protocol based on the endomorphisms ring $\mathrm{End}(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$," *Applicable Algebra in Engineering, Communications and Computing*, vol. 23(3-4), pp. 143–149, 2012.

[7] N. Koblitz, "Elliptic curve cryptosystems," *Mathematics of Computation*, vol. 48(177), pp. 203–209, 1987.

[8] M. Maze, C. Monico, J. Rosenthal, "Public Key Cryptography based on Semigroup Actions," *Advances in Mathematics of Communications*, vol. 1(4), pp. 489–507, 2007.

[9] A.J. Menezes, Y.H. Wu, "The discrete logarithm problem in $GL(n, q)$," *Ars Combinatoria*, vol. 47, pp. 23–32, 1997.
[10] V. Miller, "Use of Elliptic curves in Cryptography," *Advances in Cryptography – CRYPTO'85*, vol. 218, *Lecture Notes in Computer Science*, pp. 417–426. Springer-Verlag, New York, NY, 1986.
[11] A.G. Myasnikov, V. Shpilrain, A. Ushakov, "Group-based cryptography," Birkhäuser Verlag, 2008.
[12] R.W.K. Odoni, V. Varadharajan, P.W. Sanders, "Public key distribution in matrix rings," *Electronics Letters*, vol. 20, pp. 386–387, 1984.
[13] R.L. Rivest, A. Shamir, L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of ACM*, vol. 21(2), pp. 120–126, 1978.
[14] T. Satoh, K. Araki, "On construction of signature scheme over a certain non-commutative ring," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, 80(1), pp. 40–45, 1997.
[15] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM Journal on Computing*, 26(5), pp. 1484–1509, 1997.
[16] E. Stickel, "A new method for exchanging secret keys," *Proceedings of the Third International Conference on Information Technology and Applications (ICITA'05),* Sidney, 2005, pp. 426-430.