FACULTAD
DE
CIENCIAS

CRIPTOGRAFÍA MULTIVARIABLE

(MULTIVARIATE CRYPTOGRAPHY)

Trabajo de fin de Grado
para acceder al

GRADO EN MATEMÁTICAS

Autor: Alvaro Díez Lois

Director: Daniel Sadornil Renedo

Septiembre-2020

Índice general

Agradecimientos **III**

Resumen **V**

Introducción **1**

1. Resultados básicos de álgebra abstracta **5**
1.1. Cuerpos finitos 5
1.2. Producto tensorial 8

2. Criptografía Multivariable **11**
2.1. Criptosistemas multivariables 11
2.2. Seguridad de los MPKC's 18
2.3. Primeros intentos de MPKC's 19
2.4. Construcciones cuadráticas 20

3. Criptosistema de Matsumoto-Imai **23**
3.1. Construcción de MI 26
3.2. Matsumoto-Imai de varias ramas 29

4. Ataque por ecuaciones de linealización **31**
4.1. Dimensión del espacio de linealización para MI 32
4.2. Construcción de las ecuaciones de linealización 44
4.3. Ejemplo de un ataque por linealización 45

Bibliografía **49**

Agradecimientos

En primer lugar, quiero agradecer, a mi director Dani, por toda la paciencia que has tenido conmigo durante este año y por tu ayuda con el TFG.

Quiero agradecer también a mi familia, mi padre, mi madre y mi hermana Eva, ya que en unas circunstancias tan excepcionales como han sido estos meses debido a la pandemia con confinamiento incluido, han estado apoyándome para acabar este grado que tanto se me ha atascado al final. También a Connie, que en este último año ha estado día tras día ya sea en España o en Estados Unidos detrás de mí.

Por último, a todos mis amigos de tanto dentro como fuera de la facultad, con los que durante estos años de carrera, he compartido grandes momentos.

Resumen

Los criptosistemas multivariables utilizan técnicas de criptografía de clave pública. Debido a la aparición de los ordenadores cuánticos, la seguridad de muchos criptosistemas se ha puesto en duda, como por ejemplo el RSA, debido a la capacidad de factorizar enteros en tiempo polinomial. Estos criptosistemas están basados en la dificultad de resolver sistemas de ecuaciones polinomiales multivariables de grado mayor que 1. A lo largo del trabajo estudiaremos algunas de las características básicas de estos sistemas, así como introduciremos el primero propuesto por Matsumoto e Imai en 1988. Además, estudiaremos uno de los ataques a estos criptosistemas, el ataque basado en ecuaciones de linealización.

Palabras clave: Criptosistemas multivariables, criptografía de clave pública, sistemas de ecuaciones polinomiales multivariables, aplicación afín, cuerpo finito, extensión, ecuación de linealización

Abstract

Multivariate cryptosystems use techniques of public key cryptography. Because of the quantum computers, the security of many cryptosystems have been threatened, one example is the RSA, because that computers are able to factorize integer numbers in polynomial time. These cryptosystems are based in the difficulty of solving systems of multivariate polynomial equations of degree greater than 1. During these bachelor thesis we will study some of the basic characteristics of these systems, we will also introduce the first one proposed by Matsumoto and Imai in 1988. Besides, we will study one of the most famous attacks to these cryptosystems, the attack based on linearization equations.

Key words: Multivariate cryptosystems, public key cryptography, systems of multivariate polynomial equations, affine application, finite field, extension, linearization equation.

Introducción

La criptografía es el arte o técnica de la ocultación de mensajes. A lo largo de la historia numerosas civilizaciones han utilizado diferentes técnicas de ocultación de mensajes con el fin de que enemigos o gente ajena a ellos pudiera leer o escuchar la información contenida en ellos. Se han ido desarrollando diferentes tipos de sistemas criptográficos que emplean técnicas matemáticas para cifrar los mensajes. Uno de los más clásicos son los cifrados por sustitución monoalfabética donde el cifrado de mensajes consiste en una permutación de las letras del alfabeto de un determinado idioma. Un caso particular es el cifrado de César donde previamente se identifica cada caracter de un alfabeto con un elemento de $\mathbb{Z}/m\mathbb{Z}$ siendo m el número de caracteres del mismo. Y tomando un entero n se cifra cada letra realizando la operación modular $a + n \ mod \ m$.

Asimismo, uno de los sistemas más famosos para cifrar mensajes lo encontramos en la Máquina Enigma. Ésta era utilizada por el ejército alemán durante la Segunda Guerra Mundial para cifrar sus mensajes, para que, los ejércitos aliados, al espiar los canales de comunicación alemanes, no pudieran conocer el verdadero significado de la información intercambiada ya que se encontraba cifrada. La técnica de encriptación que empleaba Enigma era un cifrado por sustitución polialfabética. Donde para cifrar cada letra se empleaba una permutación del alfabeto distinta. Tal era la importancia de la criptografía durante la IIWW que hay expertos que aseguran que la 'ruptura' de Enigma, por parte de científicos británicos, acortó la guerra dos años más de lo previsto.

Un criptosistema está compuesto de los siguientes elementos:

- Un conjunto finito $\mathcal{A}$ llamado alfabeto que contiene todos los caracteres de un determinado idioma.
- Un conjunto $\mathcal{K}$ formado por todas las posibles claves de cifrado y descifrado.
- El conjunto formado por todas las funciones de cifrado y descifrado $\mathcal{F} : \mathcal{A} \times \mathcal{K} \longrightarrow \mathcal{A}$.

Detallemos ahora su funcionamiento:
Ana y Bob quieren mandarse mensajes sin que nadie más pueda conocer el contenido. Sea $M = (m_1, ..., m_n) \in \mathcal{A}^n$ el mensaje que Ana quiere enviar. Para ello, tomando una clave k contenida en $\mathcal{K}$ que han acordado previamente, calcula $\mathcal{F}_1(M, k)$ dando lugar al mensaje cifrado C. Ana envía el mensaje cifrado a Bob. Bob ansioso por conocer el contenido del mensaje, a partir de la clave de descfrado k' (que no tiene que ser necesariamente igual que k) calcula $\mathcal{F}_2(C, k')$ llegando al contenido original del mensaje.

Hemos resaltado como las claves de cifrado y descifrado no tienen porque ser las mismas. Añadamos un pequeño detalle, a priori no sabemos la dificultad que conlleva obtener una clave a partir de la otra. Como consecuencia de ésto, dividiremos la criptografía en dos grandes tipos:

- **Criptografía simétrica o de clave privada**: Aquella donde la clave es privada, y solo accesible a los usuarios. En este caso la claves de cifrado y descifrado o son iguales o se puede obtener una a partir de otra de manera sencilla.
- **Criptografía asimétrica o de clave pública**: Cada usuario dispone de dos claves, una pública, accesible a cualquier persona que se utiliza para cifrar. Y una privada, utilizada para descifrar mensajes y que no necesita propagarse. Obtener la clave privada conociendo únicamente la pública supone un problema prácticamente inabordable.

Cronológicamente apareció primero la criptografía de clave privada, en la que además, en gran parte de los casos las funciones de cifrado y descifrado eran idénticas. Uno de los principales problemas que surgía como consecuencia de ésto, era que dicha clave debía ser conocida por todos los usuarios del criptosistema. Y esto nos hace preguntarnos, ¿qué sucedería si durante la transmisión de la clave entre usuarios, ésta era interceptada por un enemigo? En ese caso, el sistema de cifrado sería completamente vulnerable y no aseguraría la seguridad de las comunicaciones.

Como solución al problema del intercambio de claves, surge en 1975 la criptografía de clave pública. Estos criptosistemas cambiarían los sistemas modernos de comunicación. En ellos cada usuario dispondrá de una clave pública al alcance del público general y una privada. Volvamos a utilizar a Ana y a Bob para explicar el funcionamiento de estos sistemas. Ana quiere enviar un mensaje a Bob y que su contenido sea inaccesible para cualquier agente externo a ellos. Utiliza la clave pública de Bob para cifrar el mensaje, y éste para descifrarlo, únicamente tendrá que utilizar su clave privada (solo conocida por él) y así conocer el contenido original del mensaje.

Para garantizar la seguridad en las comunicaciones al cifrar mensajes empleando técnicas de criptografía de clave pública, Whitfield Diffie y Martin Hellman propusieron en 1976 [3] una serie de condiciones que debía cumplir todo criptosistema de clave pública para ser considerado como tal. Para ello, notemos como k_b y k_v a las claves pública y privada respectivamente. Y como $\mathcal{C}$ y $\mathcal{D}$ a los conjuntos de las funciones de cifrado y descifrado respectivamente. Las condiciones son las siguientes:

1. *Sea M un mensaje en claro, $\mathcal{D}(\mathcal{C}(M, k_b), k_v) = M$.*
2. *Conocidas k_b y k_v las operaciones de cifrado y descifrado son computacionalmente sencillas.*
3. *Disponiendo únicamente de la clave pública k_b el descifrado de mensajes supone un problema de dificultad muy elevada.*

4. Es fácil determinar ambas claves k_b y k_v.

La criptografía de clave pública trajo además la posibilidad de firmar digitalmente los mensajes. Ésto facilitaría la posibilidad de confirmar la identidad del emisor. La posibilidad de cifrar mensajes está al alcance de un gran número de personas ya que la clave de cifrado como ya hemos comentado es pública. El proceso es sencillo, consiste en que el emisor utilizando sus claves privadas firma el mensaje, y una vez llegue al receptor, éste simplemente aplicará la clave pública del emisor conocida por todos para corroborar la identidad del emisor.

Actualmente, uno de los sistemas más famosos que emplean criptografía clave pública, es el algoritmo RSA, propuesto por Rivest, Shamir y Adleman en 1979 [16]. Éste basa su seguridad en la inexistencia de algoritmos capaces de factorizar números enteros grandes en tiempo polinomial. La aparición de los ordenadores cuánticos, puso en jaque a numerosos criptosistemas de clave pública, especialmente a RSA, ya que estos ordenadores son capaces de factorizar enteros en tiempo polinomial. Esto concluye en la aparición de la criptografía post-cuántica, que desarrolla algoritmos resistentes a ataques efectuados con ordenadores cuánticos, como el algoritmo de Shor [7]. Uno de los algoritmos que surgieron como consecuencia de la aparición de estos ordenadores, son los basados en sistemas de ecuaciones polinómicas multivariables, que denominaremos como Criptosistemas Multivariables, y que serán el objeto de estudio en este TFG. Su seguridad se basa en que generalmente, resolver un sistema de ecuaciones polinómicas en muchas variables, es un problema muy difícil de resolver computacionalmente [4]. Si lo miramos desde el punto de vista de la teoría de la complejidad diremos que es un problema NP-Duro.

El esquema básico de este problema consistirá en lo siguiente: se toma una función F cuyas componentes son polinomios en n variables que toman coeficientes en un cuerpo finito. Dicha función está escogida a propósito para que calcular tanto $F(x)$, como $F^{-1}(x)$ sean cálculos 'sencillos'. A continuación, se construyen dos aplicaciones afines (L_1, L_2) que 'esconderán la función fácil'. Lo harán, componiendo F con L_1 y L_2. Dando una función para la cual calcular la inversa de cualquier elemento, proceso para el cual debemos resolver un sistema de ecuaciones o calcular la inversa explícita de la función, supone un problema prácticamente inabordable.

En el capítulo 1 daremos una serie de resultados sobre cuerpos finitos. Al trabajar con polinomios sobre cuerpos finitos, necesitamos conocer una serie de nociones y resultados sobre ellos, que hasta entonces no hemos visto. Además, en una de las demostraciones que veremos a lo largo del trabajo, empleamos el producto tensorial, por tanto, daremos a conocer en que consiste, así como definiremos alguna propiedad asociada al mismo.

El capítulo 2 introduce a los Criptosistemas Multivariables. En primer lugar, describiendo su esquema básico, sus claves, como cifra, descifra y también como se pueden firmar mensajes. Además estudiaremos su seguridad y unas primeras construcciones que resultaron poco existosas. Por último, explicaremos porque los polinomios que forman las aplicaciones de los MPKC, son de grado dos.

Después de dar un esquema básico, en el capítulo 3, explicaremos en que consiste el criptosistema de Matsumoto e Imai, fue el primer criptosistema multivariable que resultó existoso en su momento. Esto éxito se vino abajo cuando Patarin, descubrió un ataque que podía romperlo [14].

Este ataque es el objeto de estudio del capítulo 4, lo conocemos como ataque por ecuaciones de linealización. A lo largo del capítulo, introducimos las ecuaciones de linealización, vemos que forman un espacio vectorial, y calculamos la dimensión de este espacio. Para ver su funcionamiento mejor, daremos un ejemplo de como se rompe un criptosistema utilizando ecuaciones de linealización.

Para la realización del trabajo nos hemos apoyado fundamentalmente en [4], apoyándonos para cuestiones más puramente matemáticas en [19].

Capítulo 1

Resultados básicos de álgebra abstracta

Antes de empezar a desarrollar el trabajo en profundidad vamos a introducir una serie de definiciones y resultados matemáticos ya vistos a lo largo del grado pero que nos serán imprescindibles en a lo largo del TFG. Algunas demostraciones serán omitidas por haber sido vistas en las asignaturas Álgebra Lineal I y II, Teoría de Galois o Álgebra Conmutativa. Muchos de estos resultados los encontramos en [6].

1.1. Cuerpos finitos

Definición 1.1 *Sea $(K, +, \cdot)$ un conjunto de q elementos dotado de las operaciones suma $+$ y multiplicación $\cdot$. Se dice que K es un cuerpo finito si cumple:*

- *$(K, +)$ es grupo abeliano*
- *$(K^*, \cdot)$ es un grupo abeliano*

En lo que sigue denotaremos al cuerpo finito de q elementos como $\mathbb{F}_q$.

Proposición 1.2 *Sea $\mathbb{F}_q$ un cuerpo finito de cardinal q, entonces $q = p^m$ donde p es primo y m es un entero positivo.*

Teorema 1.3 *Sea $\mathbb{F}_q$ un cuerpo finito, entonces el grupo multiplicativo $\mathbb{F}_q^*$ es un grupo cíclico.*

Demostración: Sea $(\mathbb{F}_q^*, \cdot)$ el grupo multplicativo del cuerpo $\mathbb{F}_q$. Aplicando el Teorema de Clasificación de los Grupos Abelianos [17,Teorema 3.] tenemos que

$$\mathbb{F}_q^* \cong (\mathbb{Z}/d_1\mathbb{Z} \times ... \times \mathbb{Z}/d_r\mathbb{Z}, +) \tag{1.1}$$

donde $d_1 > 1$ y para cada $i = 1, ..., r-1$, d_i divide a d_{i+1}. Además, $q - 1 = d_1 \cdot ... \cdot d_r$. Luego si tomamos un elemento $a \in \mathbb{F}_q^*$ de orden t, por la construcción de los d_i, sabemos que t divide a d_r. Entonces, podremos afirmar que a es raíz del polinomio

$$x^{d_r} - 1 = 0$$

Como este polinomio tiene d_r raíces (lo demostramos posteriormente en el Lema 1.6), y hemos visto que todo elemento de $\mathbb{F}_q^*$ es raíz del mismo, concluimos que

$$|\mathbb{F}_q^*| = q - 1 \leq d_r$$

Y por otro lado dado que $q - 1 = d_1 \cdot ... \cdot d_r$, d_r divide a $q - 1$, luego $q - 1 \geq d_r$. Por tanto, se tiene que $q - 1 = d_r$ y

$$\mathbb{F}_q^* \cong \mathbb{Z}/d_r\mathbb{Z}$$

Dado que $(\mathbb{Z}/d_r\mathbb{Z}, +)$ es cíclico, queda probado que el grupo multiplicativo $(\mathbb{F}_q^*, \cdot)$ es cíclico. □

Corolario 1.4 *Sea $\mathbb{F}_q$ un cuerpo finito, entonces para todo elemento $x \in \mathbb{F}_q$ se cumple*

$$x^q = x$$

Demostración: Sea $b \in \mathbb{F}_q^*$, como $(\mathbb{F}_q^*, \cdot)$ es cíclico, $b = a^i$, siendo a el generador de $\mathbb{F}_q^*$. Además por ser cíclico y tener q elementos, se tiene que $a^q = a$. Entonces

$$b^q = a^{iq} = (a^q)^i = a^i = b$$

□

Además al margen de estos tres últimos resultados básicos de cuerpos finitos, vamos a enunciar un Lema muy importante de cara a la seguridad de los Criptosistemas Multivariables ya que nos dará una idea del número de posibles claves privadas distintas.

Lema 1.5 *Sea $\mathbb{F}_q$ un cuerpo de $q = p^m$ elementos, entonces*

$$|GL(n, \mathbb{F}_q)| = \prod_{i=0}^{n-1} (q^n - q^i)$$

donde $GL(n, \mathbb{F}_q) = \{A \in \mathcal{M}_{n\times n}(\mathbb{F}_q) : det(A) \neq 0\}$

Demostración: Veamos la cantidad de matrices distintas de dimensión $n \times n$ con determinante no nulo que podemos construir. Vamos a ver cuantos vectores posibles hay por cada fila de la matriz. En la primera fila podemos introducir el vector que queramos a excepción del vector nulo, luego tendremos $q^n - 1$ posibilidades. Para la segunda fila, podremos introducir todos los vectores posibles a excepción de una combinación lineal de la primera fila, es decir, sea v la primera fila de la matriz, la segunda fila podrá estar compuesta de cualquier vector w de longitud n a excepción de λv para todo $\lambda \in \mathbb{F}_q$. Luego tendremos $q^n - q$ posibles vectores para la segunda fila.
Apliquemos un razonamiento inductivo para la i-ésima fila, sea V el subespacio generado por los vectores correspondientes a las $i - 1$ primeras filas, como por construcción sabemos que los $i - 1$ vectores son linealmente independientes, entonces $|V| = q^{i-1}$. Por tanto, para

la i-ésima fila tendremos $q^n - q^{i-1}$.
Si multiplicamos todas las posibilidades para cada fila obtenemos que tenemos

$$\prod_{i=0}^{n-1}(q^n - q^i)$$

posibles matrices $n \times n$ de determinante no nulo. □

Enunciaremos también otro resultado vital de cara a los ataques a los MPKC's, que nos dará el número máximo de soluciones de una ecuación del tipo $x^k = a$ en un cuerpo finito.

Lema 1.6 *Sea $\mathbb{F}_q$ un cuerpo finito, sea k un entero y sea $a \in \mathbb{F}_q$. Entonces se cumple que la ecuación $x^k = a$ tiene como mucho $mcd(k, q-1)$ soluciones en $\mathbb{F}_q$.*

Demostración: Empecemos con el caso trivial, dado $a = 0$, entonces la única solución es $x = 0$, luego cumple la condición.
Ahora sea el caso general, supongamos $a \neq 0$, luego la solución $x = 0$ no podrá darse. Ahora consideremos $d = mcd(k, q-1)$, por la identidad de Bezout tenemos que existen enteros α, β tales que $\alpha k - \beta(q-1) = d$. Entonces haciendo un pequeño cálculo tenemos que

$$x^k = a \iff x^{k\alpha} = a^\alpha \iff x^{d+\beta(q-1)} = a^\alpha$$

Y si aplicamos el Corolario anterior llegaremos a una igualdad de la siguiente forma

$$x^d = a^\alpha \tag{1.2}$$

Tenemos una ecuación equivalente a la anterior, debido a que toda ecuación de grado n en un cuerpo tiene n soluciones, entonces la ecuación (1.2) tendrá como mucho d soluciones en $\mathbb{F}_q$. □

Definición 1.7 *Dados dos cuerpos F, K, decimos que F es una extensión de K cuando K es un subcuerpo de F. Se cumple que $1_F = 1_K$. Además F tiene estructura de espacio vectorial sobre K. Lo denotaremos por F/K y se define el grado de la extensión como la dimensión del K-espacio vectorial que notaremos por $[F : K]$.*
Una extensión es finita cuando su grado es finito.

Definición 1.8 *Una extensión F/K se dice algebraica, si todo elemento $a \in F$ es raíz de un polinomio no nulo en $K[x]$*

Teorema 1.9 *Sea F/K una extensión, sea $(f(x))$ el ideal generado por el polinomio $f(x)$ y sea $u \in F$ un elemento algebraico sobre K, se cumple lo siguiente:*

1. *$K[u] = K(u) \approx K[x]/(f(x))$ donde $f(x) \in K[x]$ es un polinomio de grado $n \geq 1$, irreducible, mónico y $f(u) = 0$.*
2. *$\{1, u, ..., u^{n-1}\}$ es una base de $K(u)/K$ y $[K(u) : K] = n$*

Definición 1.10 *Sea F una extensión de grado n sobre K con base $\{1, u, ..., u^{n-1}\}$ y sea K^n su correspondiente espacio vectorial. Definimos la biyección canónica entre F y K^n como la aplicación $\phi : F \longrightarrow K^n$ definida de la siguiente manera:*

$$\phi(a_0 + a_1u + ... + a_{n-1}u^{n-1}) = (a_0, a_1, ..., a_{n-1})$$

Es obvio ver que se trata de una biyección y que su inversa la podemos definir de manera sencilla como

$$\phi^{-1}(a_0, a_1, ..., a_{n-1}) = a_0 + a_1u + ... + a_{n-1}u^{n-1}$$

1.2. Producto tensorial

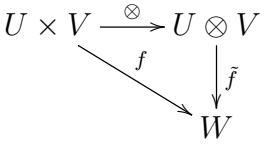
Vamos a introducir el concepto de producto tensorial, una herramienta que nos servirá más adelante para demostrar el resultado más importante de todos los que veremos en el trabajo. Hemos sacado esta información [10]. Damos por conocida la noción de aplicación bilineal, estudiada en la asignatura Álgebra Lineal II.

Definición 1.11 *Sean U y V dos $\mathbb{K}$-espacios vectoriales, se define como espacio vectorial libre T generado por $U \times V$ al formado por todas las aplicaciones bilineales $f : U \times V \longrightarrow \mathbb{K}$, tales que el conjunto $\{f^{-1}(\mathbb{K}^*)\}$ es finito.*

Definición 1.12 *Sean U y V dos espacios vectoriales, el producto tensorial entre U y V es un espacio vectorial que denotaremos $U \otimes V$, donde $\otimes$ es una aplicación bilineal:*

$$\otimes : U \times V \longrightarrow U \otimes V$$

tal que dado W otro espacio vectorial para cada aplicación bilineal $f : U \times V \longrightarrow W$, existe una única aplicación lineal $\tilde{f} : U \otimes V \longrightarrow W$ tal que $f = \tilde{f} \circ \otimes$. Es decir, que hace el siguiente diagrama conmutativo



El producto tensorial de dos espacios vectoriales se define para transformar las aplicaciones bilineales entre el producto cartesiano entre dos espacios vectoriales, en aplicaciones lineales sobre $U \otimes V$. El producto tensorial existe para cualesquiera espacios vectoriales $U \times V$ y se construye de la siguiente manera.

Sea $T(U \times V)$ el espacio vectorial libre generado por $U \times V$. La base de dicho espacio vectorial viene dada por $\left\{e_{(u,v)} : (u, v) \in U \times V\right\}$, y los elementos $e_{(u,v)}$ vienen definidos de la siguiente manera

$$\begin{array}{rccl} e_{(u,v)} : & U \times V & \longrightarrow & \mathbb{K} \\ & (u', v') & \mapsto & \begin{cases} 1 & si \;\; (u', v') = (u, v) \\ 0 & en \;\; otro \;\; caso \end{cases} \end{array}$$

Consideremos a continuación N un subespacio de T generado por elementos de la siguiente forma

$$e_{(\lambda u_1+\mu u_2,v)} - \lambda e_{(u_1,v)} - \mu e_{(u_2,v)}$$
$$e_{(u,\lambda v_1+\mu v_2)} - \lambda e_{(u,v_1)} - \mu e_{(u,v_2)}$$

Y definamos el producto tensorial entre U y V como el cociente T/N, es decir,

$$U \otimes V = T/N$$

Es de fácil comprobación que cumple la definición de producto tensorial. Dicha comprobación podemos verla en [10].

Además, éste es único salvo isomorfismo. Sean $\otimes$ y $\tilde{\otimes}$ dos productos tensoriales distintos . Dado que $U \otimes V$ y $U\tilde{\otimes}V$ son espacios vectoriales y siguiendo la definición de producto tensorial, ambos cumplen los siguientes diagramas conmutativos

$$\begin{array}{ccc} U \times V & \xrightarrow{\otimes} & U \otimes V \\ & \searrow^{\tilde{\otimes}} & \downarrow{\scriptstyle \tilde{\phi}} \\ & & U\tilde{\otimes}V \end{array} \qquad \begin{array}{ccc} U \times V & \xrightarrow{\tilde{\otimes}} & U\tilde{\otimes}V \\ & \searrow^{\otimes} & \downarrow{\scriptstyle \phi} \\ & & U \otimes V \end{array}$$

Se tiene que $\tilde{\otimes} = \tilde{\phi} \circ \otimes$ y $\otimes = \phi \circ \tilde{\otimes}$, y entonces

$$\tilde{\otimes} = \tilde{\phi} \circ \phi \circ \tilde{\otimes} \Longrightarrow id_{U\tilde{\otimes}V} = \tilde{\phi} \circ \phi$$

$$\otimes = \phi \circ \tilde{\phi} \circ \otimes \Longrightarrow id_{U\otimes V} = \phi \circ \tilde{\phi}$$

Luego $U \otimes V$ y $U\tilde{\otimes}V$ son isomorfos como queríamos demostrar. Los elementos de $U \otimes V$ los denotaremos como $u \otimes v$.

Proposición 1.13 *Sean $u_1, u_2 \in U$, $v_1, v_2 \in V$ y $\lambda \in \mathbb{K}$, entonces se cumplen las siguientes propiedades:*

1. $u_1 \otimes (v_1 + v_2) = u_1 \otimes v_1 + u_1 \otimes v_2$
2. $(u_1 + u_2) \otimes v_1 = u_1 \otimes v_1 + u_2 \otimes v_1$
3. $\lambda u_1 \otimes v_1 = u_1 \otimes \lambda v_1 = \lambda(u_1 \otimes v_1)$

Demostración: Es trivial ver que se cumplen las tres propiedades, por la construcción del producto tensorial como el espacio cociente T/N. □

La última herramienta necesaria del producto tensorial para el desarrollo del trabajo será conocer una base para el espacio vectorial $U \otimes V$.

Proposición 1.14 *Sea $U \otimes V$ el producto tensorial de los espacios vectoriales U y V. Y sean $\{u_1, \ldots, u_n\}$, $\{v_1, \ldots, v_m\}$ bases de U y V respectivamente. Entonces el conjunto*

$$\{u_i \otimes v_j : i = 1, \ldots, n \ \wedge \ j = 1, \ldots, m\}$$

es una base para $U \otimes V$.

Demostración: Para ver que $U \otimes V$ tiene como base $A = \{u_i \otimes v_j : i = 1, \ldots, n \ \wedge \ j = 1, \ldots, m\}$, veamos en primer lugar que dicho conjunto es sistema generador de $U \otimes V$, y después que tiene dimensión nm. Luego sea $u = \lambda_1 u_1 + \ldots + \lambda_n u_n \in U$ y $v = \mu_1 v_1 + \ldots + \mu_m v_m \in V$, el vector $u \otimes v$ lo podemos escribir como $(\lambda_1 u_1 + \ldots + \lambda_n u_n) \otimes (\mu_1 v_1 + \ldots + \mu_m v_m)$. Si aplicamos las propiedades descritas en la proposición anterior llegamos a que podremos expresar $u \otimes v$ de la siguiente manera

$$u \otimes v = \sum_{i=1}^{n} \sum_{j=1}^{m} \lambda_i \mu_j (u_i \otimes v_j)$$

Visto que podemos expresar $u \otimes v$ como combinación lineal de elementos en A. Veamos ahora la dimensión del espacio $U \otimes V$. Como sabemos que dos espacios tienen la misma dimensión si, y sólo si son isomorfos, vamos a probar como $U \otimes V$ es isomorfo al espacio vectorial $\mathcal{M}_{n\times m}(\mathbb{K})$ de las matrices $n \times m$ con coeficientes en $\mathbb{K}$. Sea $e_{i,j}$ la matriz con todo ceros excepto un 1 en la posición (i, j), sabemos que el conjunto $\{e_{i,j} : i = 1, \ldots, n \ \wedge \ j = 1, \ldots, m\}$ es una base para $\mathcal{M}_{n\times m}(\mathbb{K})$. Construyamos las dos siguientes aplicaciones

$$\begin{array}{rccc} \varphi: & \mathcal{M}_{n\times m}(\mathbb{K}) & \longrightarrow & U \otimes V \\ & e_{i,j} & \longmapsto & u_i \otimes v_j \end{array}$$

$$\begin{array}{rccc} f: & U \times V & \longrightarrow & \mathcal{M}_{n\times m}(\mathbb{K}) \\ & (u, v) & \longmapsto & \begin{pmatrix} \lambda_1\mu_1 & \lambda_1\mu_2 & \ldots & \lambda_1\mu_m \\ \lambda_2\mu_1 & \lambda_2\mu_2 & \ldots & \lambda_2\mu_m \\ \vdots & \vdots & \ddots & \vdots \\ \lambda_n\mu_1 & \lambda_n\mu_2 & \ldots & \lambda_n\mu_m \end{pmatrix} \end{array}$$

donde los λ_i y μ_j son los definidos con anterioridad. A continuación, y a partir de la definición de producto tensorial, sabemos que existe una única aplicación lineal $\tilde{f} : U \otimes V \longrightarrow \mathcal{M}_{n\times m}(\mathbb{K})$ que cumple que $f = \tilde{f} \circ \otimes$, es decir, $\tilde{f}(u \otimes v) = f(u, v)$. Si componemos $\tilde{f} \circ \varphi$ y $\varphi \circ \tilde{f}$ y, aplicamos las propiedades del producto tensorial y la descomposición de u y v como combinación lineal de elementos de sus bases, nos queda

$$\begin{array}{rcl} \tilde{f} \circ \varphi & = & id_{\mathcal{M}_{n\times m}(\mathbb{K})} \\ \varphi \circ \tilde{f} & = & id_{U\otimes V} \end{array}$$

Y con esto, concluimos que $\mathcal{M}_{n\times m}(\mathbb{K}) \cong U \otimes V$, luego $dim(U \otimes V) = nm$, y $\{u_i \otimes v_j\}$ es base de $U \otimes V$ como queríamos ver. $\square$

Capítulo 2

Criptografía Multivariable

En este capítulo introduciremos el tipo de criptosistemas con los que vamos a trabajar, haremos una breve introducción de por qué surgen, y luego su esquema básico que aunque ya introducimos de manera informal en la introducción del trabajo, aquí le daremos la definición formal que requiere.

2.1. Criptosistemas multivariables

Debido a la aparición de ordenadores cuánticos capaces de factorizar enteros en tiempo polinomial, la seguridad del algoritmo RSA se ve comprometida [7]. Ante este hecho, empiezan a surgir diferentes tipos de sistemas criptográficos como alternativa al mencionado RSA. Con el objetivo de dificultar el criptoanálisis y mantener la seguridad en las comunicaciones.

Estas variantes al mencionado RSA, utilizan diferentes técnicas matemáticas, las más famosas actualmente, son aquellas que se basaron en curvas elípticas. (Podemos ver una introducción básica a estas técnicas en [18]).

Aquellos que nos van a interesar, y acerca de los que profundizaremos a lo largo de la memoria, están basados en polinomios multivariables. Generalmente estos polinomios serán cuadráticos y tomarán los coeficientes en un cuerpo finito o en extensiones de cuerpos finitos. La seguridad de este tipo de sistemas reside en la dificultad de la resolución de sistemas de ecuaciones polinómicas no lineales sobre un cuerpo finito. Dentro de la criptografía multivariable encontraremos diferentes sistemas. La gran mayoría de ellos siguen un tipo de esquema de cifrado y descifrado similar, que llamaremos sistemas bipolares. Pero además, hay otro tipo de sistemas llamados sistemas mixtos, que siguen un esquema más complicado de implementar que los bipolares. Raramente han sido utilizados, pero haremos una introducción a ellos en la memoria. El más famoso lo tenemos con el sistema Dragon de Patarin [13].

Sistemas bipolares

Sea $\mathbb{F}_q$ un cuerpo finito, en este tipo de sistemas construimos una aplicación inyectiva

$$F : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^m$$

con $n \leq m$, donde cada componente de F, $f_i \in \mathbb{F}_q[x_1, ..., x_n]$. Además, dado $y = (y_1, ..., y_m) \in \mathbb{F}_q^m$, es necesario que el sistema de ecuaciones

$$F(x_1, ..., x_n) = (y_1, ..., y_m)$$

sea computacionalmente fácil de resolver. Estas aplicaciones deben ser construidas de forma que si conocemos $y = (y_1, ..., y_m)$, se puede calcular una inversa $F^{-1}(y_1, ..., y_m)$ de manera sencilla.

El siguiente paso será tomar dos aplicaciones afines biyectivas $L_1 : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^n$ y $L_2 : \mathbb{F}_q^m \longrightarrow \mathbb{F}_q^m$ escogidas al azar. Una vez presentadas estas tres aplicaciones construiremos la siguiente aplicación inyectiva

$$\overline{F} = L_2 \circ F \circ L_1$$

$$\overline{F} : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^m$$

donde $\overline{F}(x_1, ..., x_n) = (\overline{f}_1, ..., \overline{f}_m)$ y cada $\overline{f}_i \in \mathbb{F}_q[x_1, ..., x_n]$.
Las aplicaciones seguirán el siguiente diagrama conmutativo:

$$\begin{array}{ccc} \mathbb{F}_q^n & \xrightarrow{\overline{F}} & \mathbb{F}_q^m \\ \downarrow{\scriptstyle L_1} & & \uparrow{\scriptstyle L_2} \\ \mathbb{F}_q^n & \xrightarrow{F} & \mathbb{F}_q^m \end{array}$$

Pero, a diferencia de lo que sucedía para el caso de F, si tomamos $y = (y_1, ..., y_m) \in \mathbb{F}_q^m$, la resolución del sistema

$$\overline{F}(x_1, ..., x_n) = (y_1, ..., y_m)$$

deberá suponer un problema difícil de resolver computacionalmente. Podremos asumir esta afirmación, ya que actualmente los métodos conocidos para la resolución de ecuaciones polinómicas multivariables son métodos generales, como el de las bases de Groebner, el cual supone una complejidad exponencial [19].

Esto nos dará una idea de que papel jugará cada una de las aplicaciones descritas en el apartado de la generación de claves.

Generación de claves
En este tipo de sistemas, la clave pública está formada por las m componentes polinomiales de $\overline{F}$. Mientras que la clave privada, la forman las transformaciones afines L_1 y L_2. La aplicación F dependiendo del criptosistema podrá ser tanto pública como privada.

En lo sucesivo notaremos con el subíndice A a las claves del emisor y con el subíndice

B a las del receptor.

Proceso de cifrado
Ana quiere mandar un mensaje $x = (x_1, ..., x_n)$ a Bob sin que nadie pueda acceder a él. Para ello lo cifra empleando la clave pública de éste $\overline{F}_B$, es decir, calculando $\overline{F}_B((x_1, ..., x_n)) = (y_1, ..., y_m)$ para obtener el mensaje cifrado.

Tal y como hemos comentado con anterioridad, si un enemigo intercepta el mensaje cifrado, únicamente conocedor de las claves públicas de Ana y Bob, descifrar el mensaje realizando el cálculo de $\overline{F}_B^{-1}(y_1, ..., y_m)$ le conllevará un problema computacionalmente inabordable.

Proceso de descifrado
Bob recibe el mensaje, conocedor de las transformaciones afines L_{B1} y L_{B2} que forman su clave privada, sigue los siguientes pasos para descifrar el mensaje:

1. Sea $y = (y_1, ..., y_m)$ el mensaje recibido, calcula $L_{B2}^{-1}(y_1, ..., y_m)$ y como L_{B2} es biyectiva, $L_{B2}^{-1}(y_1, ..., y_m)$ es único.

2. A continuación, denotando $\overline{y} = L_{B2}^{-1}(y_1, ..., y_m)$ calcula $\overline{x} = F_B^{-1}(\overline{y})$, que como ya dijimos, se trata de un problema de fácil resolución.

3. Finalmente, calcula $x = L_{B1}^{-1}(\overline{x})$ consiguiendo el mensaje en claro.

Firma de mensajes
Para que Bob sepa que la que la ha enviado el mensaje es Ana, ésta poseedora de sus claves privadas (L_{A1} y L_{A2}) y públicas ($\overline{F}_A$), resuelve el sistema $\overline{F}_A(x) = z$, siguiendo el esquema descrito en el proceso de descifrado (normalmente z suele ser el nombre de la propia Ana o fragmentos del mensaje en claro). Obtenido $\overline{x}$ como solución al anterior sistema, ésta lo envía junto al mensaje. Así, una vez Bob haya recibido el mensaje le bastará con calcular $\overline{F}_A(\overline{x})$, obteniendo z. Esto implicará que Bob sepa con certeza que Ana es la emisora.

Proposición 2.1 *Los sistemas bipolares son un tipo de criptosistemas de clave pública.*

Demostración: Como ya explicamos antes, para que un criptosistema sea considerado de clave pública, debe cumplir las condiciones de Diffie-Hellman, así que veámoslo.

1. Consideremos M el mensaje a enviar, dividimos M en bloques de n caracteres e identificamos cada caracter con un elemento de $\mathbb{F}_q$. Luego denotemos $x = (x_1, ..., x_n) \in \mathbb{F}_q^n$ como uno de esos bloques. Cifremos x, $\overline{F}(x) = y$ donde $y \in \mathbb{F}_q^m$, por definición de $\overline{F}$ sabemos que $y = L_2(F(L_1(x)))$. Ahora debemos ver que $x = L_1^{-1}(F^{-1}(L_2^{-1}(y)))$. Como L_2 es biyectiva, $L_2^{-1}(y) = F(L_1(x))$, luego es fácil ver que

$$L_1^{-1}(F^{-1}(L_2^{-1}(y))) = L_1^{-1}(F^{-1}(F(L_1(x)))) = (L_1 \circ F \circ F^{-1} \circ L_1^{-1})(x) = id(x) = x$$

2. Conocida $\overline{F}$, es fácil el cálculo de $\overline{F}(x)$ para $x \in \mathbb{F}_q^n$, luego es fácil cifrar usando la clave pública. Y conocidas L_1, L_2 y F, calcular las inversas de L_1 y L_2 es fácil ya que se trata de resolver un sistema de ecuaciones lineales en ambos casos. Además, el cálculo de $F^{-1}(y)$ es fácil por hipótesis.

3. Si solo conocemos las componentes polinomiales de $\overline{F}$, descifrar mensajes resolviendo el sistema $\overline{F}(x) = y$ será difícil computacionalmente.

4. A partir de las claves privadas L_1, L_2 y F es fácil determinar $\overline{F}$, mediante la composición de las mismas.

□

A continuación, vamos a dar un pequeño ejemplo que nos servirá para entender mejor el funcionamiento de los sistemas bipolares. Para ello tomaremos cuerpos sencillos y parámetros pequeños que nos resulten manejables. Observaremos en este caso, como la inversa de la clave pública es fácil de calcular, pero como ya hemos dicho, se trata de un ejemplo pequeño para comprobar su funcionamiento.

Ejemplo 2.2 *Ana quiere enviar un mensaje a Bob utilizando un criptosistema bipolar. Para ello se ponen de acuerdo en tomar* $q = 7$, $n = 2$ *y* $m = 3$. *Ahora Bob construye su clave pública*

$$\overline{F} : \mathbb{F}_7^2 \longrightarrow \mathbb{F}_7^3$$

a partir de sus clave privada que consta de las tres aplicaciones siguientes:

1. $L_1 : \mathbb{F}_7^2 \longrightarrow \mathbb{F}_7^2$ *tal que dado* $(x_1, x_2) \in \mathbb{F}_7^2$, $L_1(x_1, x_2) = (2x_1 + x_2 + 1, 3x_1 + 2x_2 + 2)$

2. $L_2 : \mathbb{F}_7^3 \longrightarrow \mathbb{F}_7^3$ *tal que dado* $(x_1, x_2, x_3) \in \mathbb{F}_7^3$, $L_2(x_1, x_2, x_3) = (x_1 + x_2 + 1, x_2 + x_3 + 2, x_3 + 3)$

3. $F : \mathbb{F}_7^2 \longrightarrow \mathbb{F}_7^3$ *tal que dado* $(x_1, x_2) \in \mathbb{F}_7^2$, $F(x_1, x_2) = (x_1x_2, x_1 + x_2 + 1, x_1^2 + 2)$

Ahora componiendo las aplicaciones como indicamos anteriormente obtendrá sin ninguna dificultad $\overline{F}$ *que vendrá determinada como a continuación indicamos:*

$$\overline{F}(x_1, x_2) = (6x_1^2+2x_2^2+5x_1, 4x_1^2+x_2^2+4x_1x_2+2x_1+5x_2+2, 4x_1^2+x_2^2+4x_1x_2+4x_1+2x_2+6)$$

Ana quiere enviar el siguiente mensaje a Bob $(0, 4, 3, 3, 2, 1, 0, 6, 5, 5)$. *Primero divide el mensaje en elementos de* $\mathbb{F}_7^2$ *y ahora se dispone a cifrarlo de la forma descrita: sea* $\overline{F}$ *la clave pública de Bob. Calcula* $\overline{F}(0, 4) = (4, 3, 2)$, $\overline{F}(3, 3) = (3, 6, 0)$, $\overline{F}(2, 1) = (1, 1, 6)$, $\overline{F}(0, 6) = (2, 5, 5)$ *y* $\overline{F}(5, 5) = (1, 3, 2)$ *y le envía el mensaje cifrado* $(4, 3, 2, 3, 6, 0, 1, 1, 6, 2, 5, 5, 1, 3, 2)$.

Bob obviamente conocedor de sus claves privadas L_1, L_2 *y* F *antes de nada dividirá el mensaje en bloques de tres caracteres resultando* $(4, 3, 2) \in \mathbb{F}_7^3$, $(3, 6, 0) \in \mathbb{F}_7^3$, $(1, 1, 6) \in \mathbb{F}_7^3$, $(2, 5, 5) \in \mathbb{F}_7^3$ *y* $(1, 3, 2) \in \mathbb{F}_7^3$. *Se dispone a descifrar el mensaje siguiendo el proceso descrito anteriormente. (Realizaremos detallando paso por paso el descifrado de* $(4, 3, 2)$*)*

1. *En primer lugar, Bob calcula* $L_2^{-1}(4, 3, 2)$ *dando lugar a* $(1, 2, 6)$.

2. *A continuación, encontrará* $F^{-1}(1, 2, 6) = (5, 3)$.

3. *Por último, éste realizará el cálculo de* $L_1^{-1}(5, 3) = (0, 4)$, *siendo el primer bloque del mensaje original que Ana le había mandado.*

De manera análoga Bob descifra $(3, 6, 0)$ *dando lugar a* $(3, 3)$, $(1, 1, 6)$ *obteniendo* $(2, 1)$, $(2, 5, 5)$ *dando* $(0, 6)$ *y* $(1, 3, 2)$ *que nos dá* $(5, 5)$ *y con ello al mensaje en claro* $(0, 4, 3, 3, 2, 1, 0, 6, 5, 5)$ *que Ana le había mandado.*

Sistemas mixtos

Al igual que en los bipolares, sea $\mathbb{F}_q$ un cuerpo finito y sea $\overline{H}$ la siguiente aplicación:

$$\overline{H} : \mathbb{F}_q^{n+m} \longrightarrow \mathbb{F}_q^l$$

donde $\overline{H}(x_1, ..., x_n, y_1, ..., y_m) = (\overline{h}_1, ..., \overline{h}_l)$, y cada $\overline{h}_i$ es un polinomio en $n + m$ variables con coeficientes en $\mathbb{F}_q$.

Dicha aplicación está construida a partir de tres aplicaciones:

- Una aplicación $H : \mathbb{F}_q^{n+m} \longrightarrow \mathbb{F}_q^l$ definida de manera similar que $\overline{H}$, es decir, tomando $(x, y) = (x_1, ..., x_n, y_1, ..., y_m) \in \mathbb{F}_q^{n+m}$, $H(x, y) = (h_1, ..., h_l)$ donde cada h_i es un polinomio de $n + m$ variables con coeficientes en $\mathbb{F}_q$.

  Dado $\mathbf{x} \in \mathbb{F}_q^n$, el sistema
  $$H(\mathbf{x}, y_1, ..., y_m) = (0, ..., 0)$$
  es de fácil resolución y lineal en la mayoría de los casos.

  A su vez, dado $\mathbf{y} \in \mathbb{F}_q^m$, el sistema
  $$H(x_1, ..., x_n, \mathbf{y}) = (0, ..., 0)$$
  es fácil de resolver y no lineal.

- $L_1 \times L_2$ siendo $L_1 : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^n$ y $L_2 : \mathbb{F}_q^m \longrightarrow \mathbb{F}_q^m$ definidas igual que en el caso bipolar.

- Y $L_3 : \mathbb{F}_q^l \longrightarrow \mathbb{F}_q^l$, una aplicación lineal invertible.

Así la aplicación $\overline{H}$ quedará construida de la siguiente manera:

$$\overline{H} = L_3 \circ H \circ (L_1 \times L_2)$$

Podremos expresarla también a partir del siguiente diagrama conmutativo:

$$\begin{array}{ccc} \mathbb{F}_q^n \times \mathbb{F}_q^m & \xrightarrow{\overline{H}} & \mathbb{F}_q^l \\ \downarrow{\scriptstyle L_1 \times L_2} & & \uparrow{\scriptstyle L_3} \\ \mathbb{F}_q^n \times \mathbb{F}_q^m & \xrightarrow{H} & \mathbb{F}_q^l \end{array}$$

La construcción de $\overline{H}$ viene dada de tal forma que si desconocemos las claves privadas sea muy difícil el descifrado de mensajes únicamente a partir de la clave pública.

Al contrario que ocurría con H, en el que resolver el sistema era fácil tanto para la variable $\mathbf{x}$ como para la variable $\mathbf{y}$, la aplicación $\overline{H}$ solo permite resolver el sistema en una de las dos variables, es decir, conociendo $\mathbf{x} \in \mathbb{F}_q^n$, la resolución del sistema

$$\overline{H}(\mathbf{x}, y_1, ..., y_m) = (0, ..., 0)$$

es sencilla, mientras que conocido $\mathbf{y} \in \mathbb{F}_q^m$ la solución del sistema

$$\overline{H}(x_1, ..., x_n, \mathbf{y}) = (0, ..., 0)$$

responde a un problema inabordable computacionalmente.

Generación de claves
La clave pública está formada por las componentes polinomiales de la aplicación $\overline{H}$ y la estructura de cuerpo de $\mathbb{F}_q$. Y la clave privada la componen las dos aplicaciones afines L_1 y L_2 y la transformación lineal L_3. En los sistemas mixtos, la aplicación H es bastante indiferente si forma parte de la clave pública o privada.

Proceso de cifrado
Ana para enviar un mensaje a Bob tiene que realizar el siguiente procedimiento: sea $\mathbf{x} = (\mathbf{x}_1, ..., \mathbf{x}_n) \in \mathbb{F}_q^n$, el mensaje en claro a enviar, utilizando la clave pública de Bob ($\overline{H}_B$) resuelve el sistema $\overline{H}_B(\mathbf{x}, y_1, ..., y_m) = (0, ..., 0)$ obteniendo $\mathbf{y} = (\mathbf{y}_1, ..., \mathbf{y}_m)$ como el mensaje cifrado.

Proceso de descifrado
Una vez Bob ha recibido el mensaje, conocedor de las aplicaciones L_{B1}, L_{B2} y L_{B3} que forman su clave privada, descifra el mensaje siguiendo los siguientes pasos:

1. A partir del mensaje cifrado $\mathbf{y} = (\mathbf{y}_1, ..., \mathbf{y}_m)$, calcula $L_{B2}((y))$.

2. Resuelve el siguiente sistema de ecuaciones:

$$H_B(x_1, ..., x_n, L_2(\mathbf{y})) = (0, ..., 0)$$

   obteniendo $\mathbf{x} = (\mathbf{x}_1, ..., \mathbf{x}_n)$

3. Por último, calcula $L_{B1}^{-1}(\mathbf{x})$ obteniendo el mensaje en claro.

Firma de mensajes
Para firmar un mensaje $\mathbf{y} = (\mathbf{y}_1, ..., \mathbf{y}_m)$, Ana toma $z \in \mathbb{F}_q^m$ (z al igual que en el caso de los sistemas bipolares suele tratarse de un fragmento del propio mensaje, el nombre de Ana o algo identificativo de la misma) y resuelve el sistema

$$\overline{H}_A(x_1, ..., x_n, z) = (0, ..., 0)$$

siguiendo los mismos pasos que en el proceso de descifrado. Obtiene $\mathbf{x} \in \mathbb{F}_q^n$ y lo escribe a continuación del mensaje cifrado. Así, una vez Bob reciba el mensaje, usando la clave pública de Ana resuelve

$$\overline{H}_A(\mathbf{x}, y_1, ..., y_m) = (0, ..., 0)$$

obteniendo z. Ahora sabrá que fue Ana quien le mandó el mensaje.

Proposición 2.3 *Los sistemas mixtos son un tipo de criptosistemas de clave pública*

Demostración: Al igual que hicimos en la Proposición 2.1 para el caso de los sistemas bipolares, debemos verificar que los mixtos cumplen las condiciones de Diffie-Hellman para poder ser considerados de clave pública.

1. Sea M un mensaje en claro, dividamos el mensaje en bloques de n caracteres e identifiquemos cada caracter con un elemento de $\mathbb{F}_q$. Sea $\mathbf{x} = (\mathbf{x}_1, ..., \mathbf{x}_n) \in \mathbb{F}_q^n$ uno de esos bloques, el cifrado de $\mathbf{x}$ vendrá dado por la resolución del sistema

$$\overline{H}(\mathbf{x}_1, ..., \mathbf{x}_n, y_1, ..., y_m) = (0, ..., 0)$$

   Sea $\mathbf{y} = (\mathbf{y}_1, ..., \mathbf{y}_m) \in \mathbb{F}_q^m$ la solución a dicho sistema, entonces sabemos que por como hemos construido $\overline{H}$ que

$$L_3(H(L_1(\mathbf{x}), L_2(\mathbf{y}))) = 0$$

   Y como L_3 es una biyección, tenemos que $L_3^{-1}(0) = 0$. Descifremos ahora $\mathbf{y}$ siguiendo el proceso descrito anteriormente. Calculamos $L_2(\mathbf{y})$ y resolvemos el sistema $H(x, L_2(\mathbf{y})) = 0$, por ser H inyectiva $x = L_1(\mathbf{x})$, y finalmente,

$$L_1^{-1}(L_1(\mathbf{x})) = \mathbf{x}$$

   debido a la inyectividad de L_1. Llegando al mensaje en claro y comprobando que se cumple la primera condición de Diffie-Hellman.

2. Conociendo la clave pública $\overline{H}$ el cifrado de mensajes $\mathbf{x} \in \mathbb{F}_q^n$ resolviendo el sistema $\overline{H}(\mathbf{x}, y) = 0$ supone un problema fácil de resolver. Asimismo conocidas las claves privadas L_1, L_2, L_3 y H el cálculo de $L_2(y)$ como el de $L_1^{-1}(x)$ al tratarse de aplicaciones afines son fáciles. Además por hipótesis sabemos que el sistema $H(x, \mathbf{y}) = 0$ es de fácil resolución.

3. Solo conocida la aplicación $\overline{H}$ intentar descifrar mensajes resolviendo el sistema

$$\overline{H}(x, \mathbf{y}) = 0$$

   supone un problema de muy difícil solución por la construcción de $\overline{H}$. Luego descifrar mensajes conociendo únicamente la clave pública es un problema computacionalmente intratable cumpliendo la tercera condición de Diffie-Hellman.

4. La obtención de $\overline{H}$ mediante la composición de $L_1 \times L_2$, H y L_3 no supone ninguna dificultad.

□

Del mismo modo que hicimos con los sistemas bipolares para entender mejor el proceso de los sistemas mixtos pondremos un ejemplo sencillo utilizando el mismo cuerpo que en el Ejemplo 2.2 y tomando valores pequeños tanto para n, m y l.

Ejemplo 2.4 *Sea $q = 7$, $n = 2$, $m = 3$ y $l = 3$. Ahora construyamos la clave pública de Bob*

$$\overline{H} : \mathbb{F}_7^2 \times \mathbb{F}_7^3 \longrightarrow \mathbb{F}_7^3$$

a partir de sus claves privadas que presentamos a continuación:

1. *$L_1 \times L_2 : \mathbb{F}_7^2 \times \mathbb{F}_7^3 \longrightarrow \mathbb{F}_7^2 \times \mathbb{F}_7^3$ donde L_1 y L_2 serán las mismas que en el Ejemplo 2.2.*

2. *$H : \mathbb{F}_7^2 \times \mathbb{F}_7^3 \longrightarrow \mathbb{F}_7^3$ tal que para $(x_1, x_2, y_1, y_2, y_3) \in \mathbb{F}_7^2 \times \mathbb{F}_7^3$, $H(x_1, x_2, y_1, y_2, y_3) = (x_1x_2 + y_1 + y_2 + 1, x_1 + x_2 + 2y_2 + 2y_3 + 2, x_1^2 + y_3 + 4)$ que como vemos es lineal para y_i $i = 1, 2, 3$.*

3. *Y por último, la aplicación lineal $L_3 : \mathbb{F}_7^3 \longrightarrow \mathbb{F}_7^3$ definida de la siguiente manera: $L(y_1, y_2, y_3) = (y_1, y_2 + y_3, y_3)$*

Presentadas las tres aplicaciones y realizando la composición como indicamos llegaremos a la aplicación $\overline{H}$ definida como sigue

$$\begin{aligned}\overline{H}(x_1, x_2, y_1, y_2, y_3) =& (6x_1^2 + 2x_2^2 + 4x_2 + y_1 + 2y_2 + y_3 + 6,\\ & 4x_1^2 + x_2^2 + 4x_1x_2 + 2x_1 + 5x_2 + 2y_2 + 5y_3 + 2,\\ & 4x_1^2 + x_2^2 + 4x_1x_2 + 4x_1 + 2x_2 + y_3 + 1)\end{aligned}$$

Supongamos que Ana quiere mandar el mismo mensaje que antes a Bob $(0, 4, 3, 3, 2, 1, 0, 6, 5, 5)$, pero desencantada con el funcionamiento de los sistemas bipolares decide emplear un sistema mixto. Al igual que antes, divide el mensaje en varios bloques pertenecientes a $\mathbb{F}_7^2$ para cifrarlos. Para cifrar el mensaje, utiliza la clave pública de Bob resolviendo los sistemas $\overline{H}(0, 4, y_1, y_2, y_3) = (0, 0, 0)$, $\overline{H}(3, 3, y_1, y_2, y_3) = (0, 0, 0)$, $\overline{H}(2, 1, y_1, y_2, y_3) = (0, 0, 0)$, $\overline{H}(0, 6, y_1, y_2, y_3) = (0, 0, 0)$ y $\overline{H}(5, 5, y_1, y_2, y_3) = (0, 0, 0)$ dando lugar a $(3, 5, 3)$, $(6, 2, 5)$, $(3, 2, 6)$, $(1, 1, 0)$ y $(6, 5, 3)$ respectivamente. Envía el mensaje $(3, 5, 3, 6, 2, 5, 3, 2, 6, 1, 1, 0, 6, 5, 3)$ a Bob. Y éste, conocedor de sus claves privadas previa división del mensaje en cinco elementos de $\mathbb{F}_7^3$, procede a descifrarlo según el proceso indicado (solo se detallará el descifrado del primer bloque $(3, 5, 3)$:

1. *Primero calcula $L_2(3, 5, 3) = (2, 3, 6)$*

2. *Resuelve el sistema $H(x_1, x_2, 2, 3, 6) = (0, 0, 0)$ obteniendo como solución $(5, 3)$.*

3. *Para finalizar, calcula $L_1^{-1}(5, 3) = (0, 4)$ que era el mensaje que Ana le había enviado.*

De manera análoga Bob descifra $(6, 2, 5)$, $(3, 2, 6)$, $(1, 1, 0)$ y $(6, 5, 3)$ obteniendo la parte del mensaje resultante $(6, 2, 5, 3, 2, 6, 1, 1, 0, 6, 5, 3)$. Ahora ya conoce el contenido del mensaje que Ana le había mandado $(0, 4, 3, 3, 2, 1, 0, 6, 5, 5)$.

2.2. Seguridad de los MPKC's

Una vez presentados los criptosistemas multivariables, queremos ver la seguridad de los mismos, es decir, asegurarnos que al cifrar nuestros mensajes con un sistema de este tipo nos aseguraremos que el contenido del mismo solo pueda ser accesible al destinatario del mensaje.

Un posible primer ataque a los MPKC, sería utilizando métodos de 'fuerza bruta', es decir,

intentando comprobar una a una las distintas posibilidades que tenemos de clave privada, hasta ver si damos con la correcta. Al estar compuesta la clave privada de aplicaciones afines y lineales invertibles, podemos aproximar este número viendo el número de matrices invertibles distintas de tamaño $n \times n$. Este número viene dado en el Lema 1.5. Si tenemos un sistema con unos parámetros q y n grandes, el producto

$$\prod_{i=0}^{n-1}(q^n - q^i)$$

será un número muy elevado, por lo que comprobar para cada aplicación afín, las posibles matrices asociadas una a una, nos llevará un tiempo altísimo. Luego, podemos decir que estos criptosistemas son resistentes a ataques por fuerza bruta.

Al tratarse de un sistema basado en la criptografía de clave pública, cifrar mensajes está al alcance de cualquier persona, es decir, las componentes polinomiales de la aplicación $\overline{F}$ son conocidas por el público. Pero como hemos visto introduciendo los sistemas bipolares, por la construcción de $\overline{F}$, el cálculo de $\overline{F}^{-1}(y_1, ..., y_m)$ resolviendo el sistema de ecuaciones $\overline{F}(x_1, ..., x_n) = (y_1, ..., y_m)$ se trata de un problema difícil de resolver. (El razonamiento es análogo para los sistemas mixtos cambiando $\overline{F}$ por $\overline{H}$).

Asimismo, debemos asegurarnos que en caso de existir la inversa explícita de la aplicación $\overline{F}$, las componentes polinomiales de ésta deberán ser de grado 'alto'. Para así, no poder determinar dichas componentes comparando textos en claro con textos cifrados mediante $\overline{F}$. Y en consecuencia, rompiendo la seguridad de los sistemas.

Por último, otro aspecto muy a tener en cuenta será la dificultad de factorizar $\overline{F}$ como la composición de la tres aplicaciones que definimos anteriormente ($\overline{F} = L_2 \circ F \circ L_1$).

2.3. Primeros intentos de MPKC's

Antes de la aparición de los primeros criptosistemas multivariables exitosos, se dieron intentos fallidos por construir sistemas parecidos a MPKC's. En 1984 se propuso el primer esquema de firma basado en criptografía multivariable, por parte de Ong, Shamir y Schnorr [12]. Consistía en la resolución de la ecuación

$$x_1^2 + kx_2^2 = m \ mod \ n$$

donde m es el mensaje, $k \in \mathbb{Z}$ y n es un entero grande difícil de factorizar. La firma de mensajes consiste en resolver la ecuación anterior dando lugar a uno de los pares (x_1, x_2) que cumplen la igualdad anterior. Es bastante fácil de ver que, conocida la factorización de n, la ecuación es fácil de resolver. Luego este criptosistema contará con n como clave pública y su factorización será su clave privada. Ésto implica que la seguridad de éste sistema se base en la dificultad de factorizar n. Por tanto, vemos grandes similitudes entre este sistema y el RSA. Además, Pollard y Schnorr consiguieron romper el criptosistema [15], con un algoritmo que permitía encontrar una solución a la ecuación para un m concreto,

desconociendo la factorización de n.

También surgieron los sistemas triangulares propuestos por Diffie y Fell [5]. Éstos se basaban en la composición de muchas aplicaciones lineales sobre $\mathbb{F}_q$ de la forma

$$T(x_1, ..., x_n) = (x_1 + g(x_2, ..., x_n), x_2, ..., x_n)$$

donde $g(x_2, ..., x_n) \in \mathbb{F}_q[x_2, ..., x_n]$. Dado un mensaje $x = (x_1, ..., x_n)$, éste se cifraba calculando $T(x_1, ..., x_n)$. Vemos fácilmente, que si g es invertible, la aplicación T también lo será. Luego conocida g el descifrado de mensajes es un cálculo sencillo. Este sistema no tuvo mucho éxito debido a que la búsqueda de una alta seguridad conlleva tratar con claves públicas de longitud muy elevada. Por tanto, muy difíciles de manejar y almacenar, lo que nos lleva a un sistema muy poco útil en la práctica.

2.4. Construcciones cuadráticas

La mayor parte de los criptosistemas les podemos agrupar dentro del los sistemas bipolares donde la función de cifrado o clave pública vendrá dada por la siguiente fórmula:

$$\overline{f}_k(x_1, ...x_n) = \sum_{1 \leq i \leq j}^{n} a_{ij} x_i x_j + \sum_{i=1}^{n} b_i x_i + c$$

donde $a_{ij}, b_i, c \in \mathbb{F}_q$. Como podemos ver cada componente de la clave pública $\overline{F}$ se trata de un polinomio multivariable de grado dos, y ahora nos preguntamos: ¿por qué polinomios de grado dos y no de superior? Esto se debe a que bucamos una clave pública que sea fácil de almacenar y transportar, así como el cifrado de mensajes mediante el cálculo de $\overline{F}(x)$ no nos suponga ninguna dificultad. Pero que a su vez sea segura, es decir, que los enemigos no puedan descifrar mensajes a partir de la clave pública. Debido a esto último descartamos los polinomios de grado 1, ya que la resolución de un sistema lineal de ecuaciones resulta un problema sencillo. Conocemos diversos métodos para resolverlos, como la factorización LU, factorización de Cholesky, método de Jacobi, etc. Como bien explica [19], la elección ideal es grado dos ya que escogiendo un número de variables razonable, resolver sistemas de ecuaciones con polinomios de grado dos, supone ya un problema de complejidad NP-Duro. Escoger grados superiores a dos lo único que hará es hacer más lento el proceso de cifrar mensajes, y la seguridad del sistema apenas variará.

Proposición 2.5 *La longitud de las claves públicas de los criptosistemas que utilizan construcciones cuadráticas viene dada por la fórmula:*

$$\begin{cases} m(\frac{n(n+1)}{2} + n + 1) & si \quad q \neq 2 \\ m(\frac{n(n-1)}{2} + n + 1) & si \quad q = 2 \end{cases}$$

Demostración: Tomemos $\overline{F}_k$ como una de las componentes polinomiales de la clave pública. Es trivial ver que tenemos 1 término de grado 0, c, y n términos de grado 1. Ahora para

cada uno de los términos de grado 2, dado $i = k$, tenemos $j = n - k$ posibles términos, luego habrá

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$$

sumandos de grado 2. En los cuales, dado el caso en el que $q = 2$, se tiene que $x_i^2 = x_i$ para todo $x_i \in \mathbb{F}_2$. Por tanto, el número de sumandos de grado 2 será

$$\sum_{i=1}^{n-1} i = \frac{n(n-1)}{2}$$

□

Capítulo 3

Criptosistema de Matsumoto-Imai

Los primeros intentos de desarrollar MPKC's no resultaron existosos, ya que, o basaban su seguridad en la factorización de enteros como el esquema de firma propuesto en la sección 2.3, con lo cual no resuelven el principal problema que aquí se nos plantea, o fueron rotos con no mucha dificultad. Como consecuencia a esto, Tsutomu Matsumoto y Hideki Imai propusieron en 1988 [11] un nuevo criptosistema. A diferencia de los anteriores planteados, utilizaron la estructura de $\mathbb{F}_{q^n}$ tanto como $\mathbb{F}_q$-espacio vectorial como extensión $\mathbb{F}_{q^n}/\mathbb{F}_q$ de grado n. Para ello buscaron aplicaciones invertibles sobre $\mathbb{F}_{q^n}$ que pudieran transformarse en aplicaciones sobre $\mathbb{F}_q^n$.

A partir de éstas ideas, surgió el Criptosistema de Matsumoto e Imai mas conocido como MI. Debido a su alta seguridad y eficiencia, MI alcanzó tan relevancia que llegó a ser propuesto para formar parte de los estándares de seguridad del gobierno japonés. Sin embargo, éste fue roto justo antes de la selección final por Jacques Patarin utilizando ataques por linealización [14]. Esto nos podría hacer pensar que era el fin de MI, pero no fue así ya que Matsumoto-Imai trajo consigo una nueva idea matemática en el campo de la criptografía multivariable que fue utilizada y extendida por diferentes criptógrafos a la hora de desarrollar nuevos sistemas. Además, surgieron nuevas variantes de MI, como los esquemas de firma Sflash [1], aceptados en 2004 por el Nuevo Proyecto Europeo para Firmas, Integridad y Encriptación (NESSIE), como una de las selecciones finales para su uso en tarjetas inteligentes de bajo coste.

El objetivo principal de MI, como bien comentamos en el primer párrafo del capítulo, es buscar aplicaciones sobre $\mathbb{F}_{q^n}$ y transformarlas en otras sobre $\mathbb{F}_q^n$ que representen la misma función. Para ello, necesitaremos previamente una serie de resultados que probarán que, dada una función formada por varias componentes polinómicas multivariables de grado dos con coeficientes en $\mathbb{F}_q$, podremos representarla con un único polinomio univariado sobre $\mathbb{F}_{q^n}$.

Para poder alcanzar nuestro objetivo, como vemos en [19], debemos primero empezar por las funciones cuyas componentes polinómicas son de grado uno, que no son otras que las aplicaciones afines.

Definición 3.1 *Sean l_1,...,l_n polinomios de grado uno cuyos coeficientes son elementos de $\mathbb{F}_q$. Sea ahora $L : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^n$ una aplicación afín tal que $L(x) = (l_1(x), ..., l_n(x))$. A estos*

polinomios se les llama representación multivariable de L.

Proposición 3.2 *Sea $\mathbb{F}_{q^n}$ una extensión de grado n sobre $\mathbb{F}_q$ y sean B_i,$A \in \mathbb{F}_{q^n}$ entonces la aplicación definida como*

$$L(X) = \sum_{i=0}^{n-1} B_i X^{q^i} + A$$

es una aplicación afín de $\mathbb{F}_{q^n}$ en $\mathbb{F}_{q^n}$.

Demostración: En primer lugar, sea $X \in \mathbb{F}_{q^n}$ la aplicación $f(X) = X^q$ es lineal. Si $X = a_0 + a_1 u + ... + a_{n-1}u^{n-1}$, $X^q = a_0 + a_1 u^q + ...a_{n-1}u^{(n-1)q}$ y luego podemos expresar cada u^{iq} en función de los elementos de la base. Por tanto, es trivial afirmar que la aplicación L es una transformación afín sobre $\mathbb{F}_{q^n}$. □

Además a la representación anterior la llamaremos representación univariable de la aplicación afín L.

Una vez vistas las representaciones de una aplicación afín tanto sobre $\mathbb{F}_q^n$ como sobre $\mathbb{F}_{q^n}$, el primer paso será relacionarlas entre sí a través del siguiente lema [8].

Lema 3.3 *Una aplicación afín representada de forma multivariable puede ser transformada a una representación univariable y viceversa.*

Demostración: Para la representación multivariable, tenemos n polinomios de grado uno de n variables cada uno. Como los polinomios toman coeficientes en $\mathbb{F}_q$, para cada polinomio habrá q^{n+1} posibilidades. Luego, en total habrá $(q^{n+1})^n$ posibles aplicaciones afines sobre $\mathbb{F}_q$. En el segundo caso, tenemos q^n posibilidades para cada B_i y n sumandos, además de q^n posibilidades para A, luego habrá $(q^n)^n \cdot q^n$ posibles representaciones univariables. Por tanto, habrá el mismo número de posibles representaciones multivariables de L como de polinomios univariados.

A continuación, sean dos polinomios que representan dos aplicaciones afines cualesquiera en $\mathbb{F}_{q^n}$

$$P_1(X) = \sum_{i=0}^{n-1} B_i X^{q^i} + A$$

$$P_2(X) = \sum_{i=0}^{n-1} D_i X^{q^i} + C$$

Si restamos ambos polinomios, obtendremos uno nuevo no nulo de grado q^{n-1} que representa la aplicación nula. Luego cada elemento de $\mathbb{F}_{q^n}$ será raíz del mismo, por tanto, $P_1 - P_2$ tendrá q^n raíces lo que es una contradicción. Por ello, concluimos que cada representación multivariable tiene asociada una de una sola variable. □

Lema 3.4 *Sea $\mathbb{F}_q$ un cuerpo finito de q elementos y sea $\mathbb{F}_{q^n}$ una extensión de grado n sobre $\mathbb{F}_q$. Dado $P(X) = CX^{q^a+q^b} \in \mathbb{F}_{q^n}[x]$ para ciertos $a, b \in \mathbb{N}$, entonces existe una aplicación $F : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^n$ donde cada $f_i \in \mathbb{F}_q[x]$ es de grado dos, que calcula la misma función, es decir, para cada $Y \in \mathbb{F}_{q^n}$*

$$\phi(P(Y)) = F(\phi(Y))$$

Demostración: Descompongamos $P(X)$ en dos monomios $G(X) = CX^{q^a}$ y $H(X) = X^{q^b}$. A continuación, reduzcamos el grado de G y H identificando q^a, q^b con su correspondiente elemento en $\mathbb{Z}/(q^n-1)\mathbb{Z}$, dando lugar a $q^{a'}, q^{b'} \in \mathbb{Z}/(q^n-1)\mathbb{Z}$. Luego, $G(X) = CX^{q^{a'}}$ y $H(X) = X^{q^{b'}}$. Llegados hasta este punto, podemos observar como tanto G como H son la representación univariable de una afinidad. Por tanto, podremos aplicar el Lema 3.3 a ambos monomios, obteniendo así sus respectivas representaciones multivariables. Denotando G' a la representación multivariable de G, ésta tendrá la siguiente forma:

$$G'(x_1, ..., x_n) = (\phi \circ G \circ \phi^{-1})(x_1, ..., x_n)$$

entonces,

$$\phi \circ G = G' \circ \phi$$

Análogamente, construimos la aplicación H', y multiplicando G' y H' módulo $f(x)$, siendo este último un polinomio cualquiera con coeficientes en $\mathbb{F}_q$, y además, como $\mathbb{F}_{q^n} = \mathbb{F}_q/(f(x))$, obtenemos la representación multivariable de $P(X)$ de tal forma que

$$(\phi \circ P)(Y) = (F \circ \phi)(Y)$$

□

Veámoslo mejor con un ejemplo

Ejemplo 3.5 *Sea $q = 4$, luego $\mathbb{F}_4 = \{0, 1, \alpha, \alpha+1\}$, y sea $\mathbb{F}_{2^2}[x]/(x^3+x+1)$ como la extensión de grado $n = 3$ sobre $\mathbb{F}_{2^2}$ con base $\{1, u, u^2\}$. Sea ahora $P : \mathbb{F}_{4^3} \longrightarrow \mathbb{F}_{4^3}$ definida de la siguiente manera:*

$$P(X) = X^{4^2+4^1} = X^{20}$$

Ahora dado $X = a + bu + cu^2 \in \mathbb{F}_{4^3}$ calculemos su imagen por P,

$$P(X) = (a + bu + cu^2)^{20} = a^{20} + b^{20}u^{20} + c^{20}u^{40}$$

A partir del Corolario 1.4, y dado que u es raíz de x^3+x+1, tenemos la siguiente igualdad

$$a^{20} + b^{20}u^{20} + c^{20}u^{40} = (a^2 + b^2(u^2+1) + c^2(u^2+u+1) = (a^2+c^2) + c^2u + (b^2+c^2)u^2$$

Y aplicando ϕ nos queda

$$(a^2 + c^2, c^2, b^2 + c^2) \in \mathbb{F}_4^3$$

Ahora si definimos $F : \mathbb{F}_4 \longrightarrow \mathbb{F}_4$ como

$$F(x_1, x_2, x_3) = (x_1^2 + x_3^2, x_3, x_2^2 + x_3^2)$$

es trivial ver que si aplicamos ϕ^{-1} a F nos queda la misma función que si componemos P con F.

3.1. Construcción de MI

En lo que sigue denotaremos con letras mayúsculas a los elementos de las extensiones y con letras minúsculas a los elementos de espacios vectoriales o del cuerpo base sobre el que está tomada la extensión.

Partimos de un cuerpo finito $\mathbb{F}_q$, donde $q = 2^m$. Ahora consideramos $g(x)$ como un polinomio irreducible de grado n. Aplicando el Teorema 1.9 podemos definir $\mathbb{F}_{q^n} = \mathbb{F}_q[x]/g(x)$, como una extensión de grado n sobre $\mathbb{F}_q$. Además, como ya sabemos $\mathbb{F}_{q^n}$ tendrá también estructura de $\mathbb{F}_q$-espacio vectorial. Consideremos ϕ como la biyección canónica entre $\mathbb{F}_{q^n}$ y $\mathbb{F}_q^n$ definida en el capítulo 1.

Sea $1 \leq \theta < n$ tal que:

$$mcd(q^\theta + 1, q^n - 1) = 1$$

definiremos la siguiente aplicación $\tilde{F} : \mathbb{F}_{q^n} \longrightarrow \mathbb{F}_{q^n}$, donde dado $X \in \mathbb{F}_{q^n}$, se tiene que

$$\tilde{F}(X) = X^{q^\theta+1}$$

Una vez definida $\tilde{F}$, podemos definir de manera explícita $\tilde{F}^{-1}$. Si consideramos $h \in \mathbb{Z}$ que cumple que

$$h(q^\theta + 1) \equiv 1 \ mod \ (q^n - 1) \tag{3.1}$$

se tiene que en aplicación del Corolario 1.4 y de la propia definición de h

$$X^{h(q^\theta+1)} = X^{1+k(q^n-1)} = X \cdot (X^{q^n-1})^k = X \cdot 1^k = X$$

por ello $\tilde{F}^{-1}$ quedará definida por

$$\tilde{F}^{-1} = X^h$$

Es fácil ver que $\tilde{F}$, tiene la forma del monomio dado en el Lema 3.4, en este caso con $a = \theta$ y $b = 0$. Luego F será la representación multivariable de $\tilde{F}$

$$F = \phi \circ \tilde{F} \circ \phi^{-1}$$

Por tanto, F quedará definida por n componentes que serán polinomios de n variables que toman sus coeficientes en $\mathbb{F}_q$. Asimismo, esta aplicación será única, como bien probamos en la sección anterior.

Por último, para darle a este criptosistema la estructura de un MPKC, tomaremos dos aplicaciones afines invertibles $L_1, L_2 : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^n$ para construir la función de cifrado $\overline{F}$ al componer

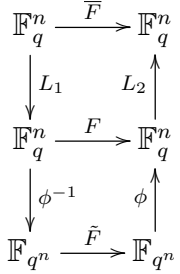
$$\overline{F} = L_2 \circ \phi \circ \tilde{F} \circ \phi^{-1} \circ L_1$$

además, podemos definirla como sigue

$$\overline{F} : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^n$$

donde $\overline{F}(x_1, ..., x_n) = (\overline{f}_1, ..., \overline{f}_n)$ y cada $\overline{f}_i \in \mathbb{F}_q[x_1, ..., x_n]$.

Por tanto, $\overline{F}$ cumple el siguiente diagrama conmutativo



Generación de claves
La clave pública se compone de la estructura de cuerpo de $\mathbb{F}_q$ y de las n componentes polinomiales de $\overline{F}$.

La clave privada está formada por las dos transformaciones afines L_1 y L_2. El parámetro θ es indiferente si forma parte de la clave pública o privada ya que al ser un número inferior a n y siendo éste último un valor 'pequeño', las posibles elecciones de θ serán reducidas. Por tanto, no tiene efecto alguno en términos de seguridad. Como el valor de θ determina $\tilde{F}$ y en consecuencia F. Éstas formarán parte de la clave pública o privada en función de que lo haga θ o no.

Proceso de cifrado
Por seguir un esquema acorde a los sistemas bipolares, ciframos un mensaje $x = (x_1, ..., x_n) \in \mathbb{F}_q^n$, calculando $\overline{F}(x_1, ..., x_n)$. Siendo $y = (y_1, ..., y_n) = \overline{F}(x_1, ..., x_n)$ el mensaje cifrado.

Proceso de descifrado
Los pasos a seguir para descifrar mensajes serán casi idénticos a los descritos en los sistemas bipolares. Únicamente tendremos que sustituir F^{-1} por $(\phi \circ \tilde{F}^{-1} \circ \phi^{-1})$. Luego, dado un mensaje cifrado $y = (y_1, ..., y_n) \in \mathbb{F}_q^n$ seguimos los siguientes pasos para descifrarlo:

1. Primero calculamos $L_2^{-1}(y_1, ..., y_n) = (\overline{y}_1, ..., \overline{y}_n)$
2. Acto seguido, calculamos $F^{-1}(\overline{y}_1, ..., \overline{y}_n) = (\phi \circ \tilde{F}^{-1} \circ \phi^{-1})(\overline{y}_1, ..., \overline{y}_n)$ que notaremos como $(\overline{x}_1, ..., \overline{x}_n)$.
3. Por último, evaluamos L_1^{-1} en $(\overline{x}_1, ..., \overline{x}_n)$ dando lugar al mensaje original.

Como su estructura se corresponde con los sistemas bipolares. MI cumple las condiciones de Diffie-Hellman y podemos considerarlo un criptosistema de clave pública.

Vamos a desarrollar un ejemplo sencillo que nos ayude a comprender con mayor exactitud como funcionan este tipo de sistemas.

Ejemplo 3.6 *En primer lugar tomemos $\mathbb{F}_{2^2}$ como cuerpo finito de cardinal $q = 2^2 = 4$ y con $ctca(K) = 2$. Los elementos de $\mathbb{F}_4$ son generados a partir de α y 1, cumpliendo la*

igualdad $\alpha^2 + \alpha + 1 = 0$. *Con ello los elementos que forman* $\mathbb{F}_{2^2}$ *serán los siguientes:*

$$\{0, 1, \alpha, \alpha + 1\}$$

Ahora consideramos $\mathbb{F}_{2^2}[x]/(x^3 + x + 1)$ *como la extensión de grado* $n = 3$ *sobre* $\mathbb{F}_{2^2}$ *con base* $\{1, u, u^2\}$. *El siguiente paso será la elección de* θ *que debido al grado de la extensión solo podrá tomar los valores* $\theta = 1$ *o* $\theta = 2$. *Para este ejemplo consideremos* $\theta = 1$.

Definidos tantos n *como* θ *y siguiendo el esquema de la construcción de MI tenemos que la aplicación* $\tilde{F} : \mathbb{F}_{4^3} \longrightarrow \mathbb{F}_{4^3}$ *vendrá definida como*

$$\tilde{F}(X) = X^5$$

Asimismo vimos previamente con detalle que tenemos una expresión explícita para la inversa de $\tilde{F}$, *viene dada por* $\tilde{F}^{-1}(X) = X^h$ *donde* h *recordemos que cumple (3.1). Luego, a partir de los valores escogidos en este ejemplo y realizando los cálculos necesarios tenemos que* $h = 284$, *y esto implica que* $\tilde{F}^{-1}(X) = X^{284}$.

Conocida $\tilde{F}$ *y su inversa, procedemos a definir las dos transformaciones afines* $L_1 : \mathbb{F}_{2^2}^3 \longrightarrow \mathbb{F}_{2^2}^3$ *y* $L_2 : \mathbb{F}_{2^2}^3 \longrightarrow \mathbb{F}_{2^2}^3$ *que forman parte de la clave privada. El desarrollo matricial de ambas aplicaciones es el siguiente:*

$$L_1(x_1, x_2, x_3) = \begin{pmatrix} 1 & 0 & \alpha \\ 0 & 1 & \alpha + 1 \\ 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} + \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}$$

$$L_2(x_1, x_2, x_3) = \begin{pmatrix} 1 & 1 & \alpha \\ \alpha & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$$

Para nuestro propósito de cifrar mensajes a partir de este criptosistema solo nos queda el cálculo de las componentes de la función $\overline{F}$ *de cifrado, para ello siguiendo el esquema de ésta seguiremos los siguientes pasos:*

- *Calculamos* $\phi^{-1} \circ Ł_1$*:*

  $$(\phi^{-1} \circ Ł_1)(x_1, x_2, x_3) = (x_1 + \alpha x_3 + 1) + (x_2 + (\alpha + 1)x_3)u + (x_1 + x_3 + 1)u^2$$

  Denotaremos por comodidad como $\tilde{X}$ *al dicho elemento resultante.*

- *Evaluamos* $\tilde{F}(\tilde{X}) = \tilde{X}^5 = \tilde{X}\tilde{X}^4$. *Entonces*

  $$\begin{aligned} \tilde{F}(\tilde{X}) =& (x_2^2 + (\alpha + 1)x_3^2 + x_1x_2 + x_2x_3 + (\alpha + 1)x_1x_3 + x_2 + (\alpha + 1)x_3) \\ &+ (x_2^2 + x_3^2 + (\alpha + 1)x_1x_3 + (\alpha + 1)x_3)u \\ &+ (x^1 + x^2 + x_3^2 + x_1x_2 + \alpha x_2x_3 + x_2 + 1)u^2 \end{aligned}$$

- *Aplicamos la biyeción canónica a* $\tilde{F}(\tilde{X})$ *obteniendo como resultado*

  $$\begin{aligned} \phi(\tilde{F}(\tilde{X})) =& (x_2^2 + (\alpha + 1)x_3^2 + x_1x_2 + x_2x_3 + (\alpha + 1)x_1x_3 + x_2 + (\alpha + 1)x_3, \\ & x_2^2 + x_3^2 + (\alpha + 1)x_1x_3 + (\alpha + 1)x_3, \\ & x^1 + x^2 + x_3^2 + x_1x_2 + \alpha x_2x_3 + x_2 + 1) \end{aligned}$$

- *Por último, calculando $L_2(\phi(\tilde{F}))$ tendremos las tres componentes de $\overline{F} = (\overline{f}_1, \overline{f}_2, \overline{f}_3)$. Éstas son las siguientes:*

$$\begin{cases} \overline{f}_1(x_1, x_2, x_3) = \alpha x_1^2 + \alpha x_2^2 + (\alpha+1)x_1x_2 + \alpha x_2x_3 + (\alpha+1)x_2 + \alpha \\ \overline{f}_2(x_1, x_2, x_3) = (\alpha+1)x_2^2 + \alpha x_1x_2 + \alpha x_1x_3 + \alpha x_2x_3 + \alpha x_2 + \alpha x_3 \\ \overline{f}_3(x_1, x_2, x_3) = x_1^2 + x_2^2 + x_3^2 + x_1x_2 + \alpha x_2x_3 + x_2 \end{cases}$$

3.2. Matsumoto-Imai de varias ramas

Un criptosistema de varias ramas es un sistema que utiliza el cifrado en bloque. Divide el mensaje en pequeños bloques de los cuales cada uno de ellos es cifrado mediante un criptosistema básico, para posteriormente, volver a juntarles dando lugar al mensaje cifrado. El proceso es sencillo, primero se permutan los caracteres del mensaje. A continuación, se divide en bloques (no necesariamente de misma longitud). Posteriormente, cada uno de esos bloques será cifrado con un criptosistema básico. Una vez cifrados los bloques por separado, se vuelven a juntar y se aplica otra permutación de los caracteres, dando lugar al mensaje cifrado. Cada uno de los criptosistemas básicos que cifran los bloques, se llaman las ramas del criptosistema.

En el caso de MI, consideremos $n = n_1 + ... + n_b$ la partición de un entero. Cada n_i representa la longitud del i-ésimo bloque. Para MI de varias ramas, las aplicaciones afines $L_1 : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^n$, y $L_2 : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^n$ ejercerán el papel de las permutaciones descritas en el párrafo anterior. A continuación, se construye $F : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^n$ compuesta por b ramas $(F_1, \ldots, F_b)$, de la forma que cada F_i es una aplicación $F_i : \mathbb{F}_q^{n_i} \longrightarrow \mathbb{F}_q^{n_i}$, y estará definida exactamente igual que definimos F en la construcción de MI. Cada una de las F_i, serán las encargadas de cifrar los bloques. Por último, construimos $\overline{F}$ como

$$\overline{F} = L_2 \circ F \circ L_1$$

En resumen, el MI de varias ramas es una generalización del MI construido en la sección anterior. En el que a diferencia del MI de una rama, dividimos el mensaje en bloques, donde cada uno de ellos será cifrado de forma distinta.

Capítulo 4

Ataque por ecuaciones de linealización

En este capítulo explicaremos como Patarin en 1995 consiguió romper el criptosistema de Matsumoto-Imai [14]. Para ello se basó en un tipo de ecuaciones llamadas de linealización que introduciremos a continuación.

Definición 4.1 *Sea $\mathcal{G} = \{g_1, ..., g_m\}$ un conjunto de n polinomios en $\mathbb{F}_q[x_1, ..., x_n]$. Una ecuación de linealización sobre $\mathcal{G}$ es un polinomio en $\mathbb{F}_q[x_1, ..., x_n, y_1, ..., y_m]$ de la forma:*

$$\sum_{i=1}^{n}\sum_{j=1}^{m} a_{ij}x_iy_j + \sum_{i=1}^{n} b_ix_i + \sum_{j=1}^{m} c_jy_j + d \tag{4.1}$$

En la que para cada $j = 1, ..., m$, si sustituimos y_j por $g_j(x_1, ..., x_n)$ obtenemos el polinomio nulo. Equivalentemente, una ecuación de linealización será de la forma

$$\sum_{i=1}^{n}\sum_{j=1}^{m} a_{ij}x_ig_j(x_1, ..., x_n) + \sum_{i=1}^{n} b_ix_i + \sum_{j=1}^{m} c_jg_j(x_1, ..., x_n) + d = 0 \tag{4.2}$$

para todo $x = (x_1, ..., x_n) \in \mathbb{F}_q^n$

Se puede comprobar trivialmente que el conjunto de ecuaciones de linealización sobre un conjunto de polinomios tiene estructura de $\mathbb{F}_q$-espacio vectorial.

En primer lugar, veamos que el polinomio nulo pertenece al conjunto de las ecuaciones de linealización. Podemos escribir el polinomio nulo como

$$\sum_{i=1}^{n}\sum_{j=1}^{m} 0x_iy_j + \sum_{i=1}^{n} 0x_i + \sum_{j=1}^{m} 0y_j + 0$$

Dicho polinomio se anula para cualquier conjunto de polinomios $\mathcal{G}$. Luego si denotamos $\mathcal{L}_\mathcal{G}$ como el conjunto de las ecuaciones de linealización $0 \in \mathcal{L}_\mathcal{G}$.
Sean dos ecuaciones distintas $M, N \in \mathcal{L}_G$ con coeficientes a_{ij}, b_i, c_j, d y $\overline{a_{ij}}, \overline{b}_i, \overline{c}_j, \overline{d}$ respectivamente. Construyamos la ecuación $M + N$, esta será de la forma

$$\sum_{i=1}^{n}\sum_{j=1}^{m}(a_{ij} + \overline{a_{ij}})x_iy_j + \sum_{i=1}^{n}(b_i + \overline{b_i})x_i + \sum_{j=1}^{m}(c_j + \overline{c}_j)y_j + (d + \overline{d})$$

Sustituyendo $g_j(x_1, ..., x_n)$ por y_j nos queda el polinomio.

$$\sum_{i=1}^{n}\sum_{j=1}^{m}(a_{ij}+\overline{a_{ij}})x_i g_j(x_1,...,x_n)+\sum_{i=1}^{n}(b_i+\overline{b_i})x_i+\sum_{j=1}^{m}(c_j+\overline{c}_j)g_j(x_1,...,x_n)+(d+\overline{d})=$$

$$=(\sum_{i=1}^{n}\sum_{j=1}^{m}a_{ij}x_i g_j(x_1,...,x_n)+\sum_{i=1}^{n}b_i x_i+\sum_{j=1}^{m}c_j g_j(x_1,...,x_n)+d)+$$

$$+(\sum_{i=1}^{n}\sum_{j=1}^{m}\overline{a}_{ij}x_i g_j(x_1,...,x_n)+\sum_{i=1}^{n}\overline{b}_i x_i+\sum_{j=1}^{m}\overline{c}_j g_j(x_1,...,x_n)+\overline{d})=0+0=0$$

Luego $M + N \in \mathcal{L}_{\mathcal{G}}$. Ahora sea $\lambda \in \mathbb{F}_q$ y sea M la ecuación de linealización anterior. Mediante un procedimiento análogo al anterior se prueba que λM es una ecuación de linealización. Luego concluimos que el conjunto de las ecuaciones de linealización sobre $\mathcal{G}$ es un $\mathbb{F}_q$-espacio vectorial. Lo dotaremos del nombre de espacio de linealización para $\mathcal{G}$.

Patarin observó que podía romper MI construyendo el espacio de linealización para el conjunto de polinomios que forman la clave pública. Para ello, conocido un mensaje cifrado $y = (y_1, ..., y_n) = (\overline{f}_1(x_1, ..., x_n), ..., \overline{f}_n(x_1, ..., x_n))$, si sustituimos cada una de las componentes del mensaje cifrado en las ecuaciones que forman el espacio de linealización de $\overline{F}$, tendremos un sistema de ecuaciones lineales en x_i, cuya solución contendrá el mensaje en claro. Con esto, quedaría cuestionada la seguridad del criptosistema de Matsumoto e Imai, ya que Patarin pondría al descubierto una forma de descifrar mensajes conociendo únicamente la clave pública, resolviendo un sistema de ecuaciones lineales, que como ya vimos en la sección 2.4, existen algoritmos para resolverlos.

Para que este ataque fuera viable, Patarin debía comprobar la cantidad de ecuaciones posibles que puede generar para un MI, es decir, la dimensión del espacio de linealización para el conjunto de polinomios $\overline{F} = \{\overline{f}_1, ..., \overline{f}_n\}$. Si disponemos de un sistema de ecuaciones con un número de soluciones muy grande, sería complicado de entre todas ellas saber cual es la correspondiente al mensaje en claro. El problema del cálculo de la dimensión del espacio de linealización es bastante reciente ya que aunque pronto se empezaron a conocer cotas para la dimensión, no fue hasta 2006 cuando Diene, Ding, Gower, Hodges y Yin [2] probaron un resultado con la dimensión exacta del espacio de linealización en función de los valores que tomen n y θ en MI.

4.1. Dimensión del espacio de linealización para MI

A priori, el conocimiento de la dimensión exacta será irrelevante siempre que obtengamos ecuaciones de linealización independientes, ya que, si tenemos suficientes ecuaciones podremos obtener mensajes en claro a partir de cifrados con el único conocimiento de la clave pública, tal como dicen en [2], "una medida de cuanto trabajo requiere el ataque". Para encontrar una primera cota para el espacio de linealización sobre las componentes de $\overline{F}$, necesitamos una serie de resultados previos, en los que utilizaremos como herramienta, la peculiar construcción de la clave pública, como composición de tres aplicaciones $\overline{F} = L_2 \circ F \circ L_1$.

Lema 4.2 *Sea $\overline{F} = L_2 \circ F \circ L_1$ la construcción de $\overline{F}$. Sean $\overline{\mathcal{L}}$ y $\mathcal{L}$ los espacios de linealización de las componentes de $\overline{F}$ y F respectivamente. Entonces*

$$dim(\overline{\mathcal{L}}) = dim(\mathcal{L})$$

Demostración: Empecemos la prueba tomando a la aplicación afín L_1 como la identidad. Luego $\overline{F} = L_2 \circ F$. L_2 por ser una transformación afín será de la siguiente forma

$$L_2(x_1, ..., x_n) = A \cdot (x_1, ..., x_n) + b$$

donde A es una matriz $n \times n$ con coeficientes $\alpha_{ij} \in \mathbb{F}_q$ y $b = (\beta_1, ..., \beta_n)$ con $b_i \in \mathbb{F}_q$. Con esto, cada componente de $\overline{F}$ será de la forma

$$\overline{f}_i(x_1, ..., x_n) = \sum_{j=1}^{n} \alpha_{ij} f_j(x_1, ..., x_n) + \beta_j$$

Ahora veamos como existe una biyección entre las ecuaciones de linealización de $\overline{F}$ y F. Por tanto, dada una ecuación para $\overline{F}$ llegaremos a una para F. Sea la siguiente ecuación de linealización para $\overline{F}$.

$$\begin{aligned} 0 &= \sum_{i=1}^{n}\sum_{j=1}^{n} a_{ij} x_i \overline{f}_j(x_1, ..., x_n) + \sum_{i=1}^{n} b_i x_i + \sum_{j=1}^{n} c_j \overline{f}_j(x_1, ..., x_n) + d = \\ &= \sum_{i=1}^{n}\sum_{j=1}^{n} a_{ij} x_i (\alpha_{ij} f_j(x_1, ..., x_n) + \beta_j) + \sum_{i=1}^{n} b_i x_i + \sum_{j=1}^{n} c_j (\alpha_{ij} f_j(x_1, ..., x_n) + \beta_j) + d = \\ &= \sum_{i=1}^{n}\sum_{j=1}^{n} a'_{ij} x_i f_j(x_1, ..., x_n) + \sum_{i=1}^{n} b'_i x_i + \sum_{j=1}^{m} c'_j f_j(x_1, ..., x_n) + d' = 0 \end{aligned} \tag{4.3}$$

De lo que se deduce una ecuación de linealización para F, siendo a'_{ij},b'_i,c'_j y d' los coeficientes para ella. Del mismo modo, a partir de la construcción de $\overline{F}$ se tiene que $F = L_2^{-1} \circ \overline{F}$. Como

$$L_2^{-1}(x) = A^{-1}x - A^{-1}b$$

siendo A una matriz $n \times n$ con coeficientes en $\mathbb{F}_q$ y $b \in \mathbb{F}_q^n$. Con esto, realizaremos un cálculo similar al anterior, para ello escribamos las componentes de F de la siguiente manera

$$f_j(x_1, ..., x_n) = \sum_{j=1}^{n} \overline{\alpha_{ij}} \overline{f}_j(x_1, ..., x_n) + \overline{\alpha_{ij}} \beta_j$$

donde $\overline{\alpha_{ij}}$ son los coeficientes de la matriz inversa de A y β_j son los coeficientes del vector b. Luego dada una ecuación de linealización para F, sustituimos f_j por su correspondiente expresión. Posteriormente, agruparemos los coeficientes de una forma similar a la anterior para así concluir en una ecuación de linealización para $\overline{F}$. Hemos llegado a una biyección entre las ecuaciones de linealización de $\overline{F}$ y F. En consecuencia, la dimensión del espacio de linealización de F y $L_2 \circ F$ es la misma.

Supongamos ahora L_2 como la identidad y consideremos $\overline{F} = F \circ L_1$. Sea una ecuación de linealización para F de la siguiente forma:

$$\sum_{i=1}^{n}\sum_{j=1}^{n} a_{ij}x_i f_j(x_1,...,x_n) + \sum_{i=1}^{n} b_i x_i + \sum_{j=1}^{m} c_j f_j(x_1,...,x_n) + d = 0$$

Por definición de ecuación de linealización, sabemos que esto se cumple para cada elemento en $\mathbb{F}_q^n$, luego, en particular para $\overline{x} = L_1(x)$.

$$\sum_{i=1}^{n}\sum_{j=1}^{n} a_{ij}\overline{x}_i f_j(\overline{x}_1,...,\overline{x}_n) + \sum_{i=1}^{n} b_i \overline{x}_i + \sum_{j=1}^{m} c_j f_j(\overline{x}_1,...,\overline{x}_n) + d = 0$$

Aplicando que $\overline{F}(x) = F(L_1(x)) = F(\overline{x})$, se tiene que

$$\sum_{i=1}^{n}\sum_{j=1}^{n} a_{ij}\overline{x}_i \overline{f}_j(x_1,...,x_n) + \sum_{i=1}^{n} b_i \overline{x}_i + \sum_{j=1}^{m} c_j \overline{f}_j(x_1,...,x_n) + d = 0$$

Por último, como $\overline{x}$ es la imagen de x por una aplicación afín, siguiendo un procedimiento similar al que utilizamos en (4.3), llegaremos a una ecuación de linealización para las componentes de $\overline{f}$.

$$\sum_{i=1}^{n}\sum_{j=1}^{n} a'_{ij}x_i \overline{f}_j(x_1,...,x_n) + \sum_{i=1}^{n} b'_i x_i + \sum_{j=1}^{m} c'_j \overline{f}_j(x_1,...,x_n) + d = 0 \tag{4.4}$$

En conclusión, partiendo de una ecuación en F hemos llegado a una en $\overline{F}$, y aplicando un procedimiento análogo al descrito anteriormente cuando se tomaba L_1 como la identidad, escribiendo $F = \overline{F} \circ L_1^{-1}$, llegaremos a que existe una biyección entre los espacios de linealización de F y de $F \circ L_1$. Con lo cual, las dimensiones de ambos espacios serán idénticas.

Una vez probado que las dimensiones del espacio de linealización para F, $L_2 \circ F$ y $F \circ L_1$ son las mismas, concluimos que

$$dim(\overline{\mathcal{L}}) = dim(\mathcal{L})$$

□

Como estamos interesados en el cálculo de la dimensión de $\overline{\mathcal{L}_{\overline{y}}}$ para un $\overline{y}$ fijo, necesitamos un resultado similar al anterior, que tenga en cuenta los espacios de linealización determinados por un $\overline{y}$ fijo.

Lema 4.3 *Sean $\overline{\mathcal{L}}$ y $\mathcal{L}$ los espacios de linealización descritos anteriormente. Sea $\overline{y} \in \mathbb{F}_q^n$ un mensaje cifrado y $\overline{z} = L_2^{-1}(\overline{y})$. Si $\overline{\mathcal{L}_{\overline{y}}}$ y $\mathcal{L}_{\overline{z}}$ son los espacios resultantes de sustituir $\overline{y}_i$ por y_i y $\overline{z}_i$ por y_i en las ecuaciones de $\overline{\mathcal{L}}$ y $\mathcal{L}$ respectivamente. Entonces:*

$$dim(\overline{\mathcal{L}_{\overline{y}}}) = dim(\mathcal{L}_{\overline{z}}) \tag{4.5}$$

Demostración: Antes hemos probado como existía una biyección entre $\overline{\mathcal{L}}$ y $\mathcal{L}$. Esto induce una biyección entre $\overline{\mathcal{L}}_{\overline{y}}$ y $\mathcal{L}_{\overline{z}}$. Dada la similitud con la prueba anterior, haremos una pequeña introducción a ella. Sea $L_2 = id$, en ese caso $\overline{z}$=$\overline{y}$, y por el lema anterior las dimensiones de los espacios de linealización de F y $F \circ L_1$ son iguales. Sea ahora $L_1 = id$, por ser $\overline{y}$ imagen de $\overline{z}$ por una aplicación afín, sus componentes estarán definidas de la siguiente manera

$$\overline{y} = \sum_{j=1}^{n} \alpha_{ij}\overline{z_i} + \beta_j$$

Ahora siguiendo un proceso análogo al que realizamos en el Lema 4.2 cuando L_1 es la identidad, se llega a que la dimensión del espacio de linealización para F y $L_2 \circ F$ es la misma. Entonces, concluimos que $dim(\overline{\mathcal{L}}_{\overline{y}}) = dim(\mathcal{L}_{\overline{z}})$. □

Esto sirvió a Patarin para, conocida la dimensión del espacio de linealización para F, conocer la dimensión para la clave pública $\overline{F}$. Con esto, Patarin comenzó a construir ecuaciones de linealización para MI a partir de $\tilde{F}$, veamos como lo hizo. Sean $X, Y \in \mathbb{F}_{q^n}$ tal que

$$Y = \tilde{F}(X) = X^{q^\theta+1}$$

Elevamos ambos lados a $q^\theta - 1$ y multiplicamos por XY resultando

$$XY^{q^\theta} = X^{q^{2\theta}}Y \Leftrightarrow XY^{q^\theta} - X^{q^{2\theta}}Y = 0$$

Definamos ahora $\tilde{R}(X, Y) \in \mathbb{F}_{q^n}[X, Y]$ tal que

$$\tilde{R}(X, Y) = XY^{q^\theta} - X^{q^{2\theta}}Y \tag{4.6}$$

Igual que hicimos en la construcción de F a partir de $\tilde{F}$ en MI, construimos R de la siguiente manera

$$R = \phi \circ \tilde{R} \circ (\phi^{-1} \times \phi^{-1})$$

Donde $R = (r_1, ..., r_n)$ y cada $r_i \in \mathbb{F}_q[x_1, ..., x_n, y_1, ..., y_n]$. De esta R se pueden determinar n ecuaciones de linealización para las componentes de F, por tanto, dado un $x \in \mathbb{F}_q^n$, $r_i(x, F(x)) = 0$ para todo $i = 1, ..., n$. Nos interesa saber si dado $\overline{y}$, sustituyendo $\overline{y}_i$ por y_i en las ecuaciones que forman R, cuantas serán linealmente independientes. Para ello sea $\overline{x}$ tal que $F(\overline{x}) = \overline{y}$, y sean X' e Y' sus equivalentes en $\mathbb{F}_{q^n}$. Entonces, X' debe ser solución de la ecuación:

$$XY'^{q^\theta} - X^{q^{2\theta}}Y' = 0 \tag{4.7}$$

y a su vez de

$$X^{q^{2\theta}-1} = Y'^{q^\theta-1} \tag{4.8}$$

Como bien sabemos, por el Lema 1.6, siempre que $Y' \neq 0$, dicha ecuación, tendrá como mucho $mcd(q^{2\theta} - 1, q^n - 1)$ soluciones. Debido a la condición sobre θ

$$mcd(q^\theta + 1, q^n - 1) = 1$$

y a la descomposición de $q^{2\theta} - 1$ como

$$q^{2\theta} - 1 = (q^\theta + 1)(q^\theta - 1)$$

concluimos que la ecuación (4.8) tendrá a lo sumo $mcd(q^\theta - 1, q^n - 1) + 1$ soluciones, si incluimos la solución trivial entre ellas. Para saber concretamente el número de soluciones para esta ecuación, probaremos el siguiente lema.

Lema 4.4 *Dados $a, b \in \mathbb{Z}$ entonces*

$$mcd(q^a - 1, q^b - 1) = q^{mcd(a,b)} - 1$$

Demostración: Sea $c = mcd(a, b)$ y sean k_a y k_b dos enteros tales que $a = k_a c$ y $b = k_b c$. Es fácil ver que $q^{mcd(a,b)} - 1$ divide a $q^a - 1$ y $q^b - 1$.

$$q^a - 1 = (q^c - 1)(q^{a-c} + q^{a-2c} + ... + q^{a-(k_a-1)c} + 1)$$

$$q^b - 1 = (q^c - 1)(q^{b-c} + q^{b-2c} + ... + q^{b-(k_b-1)c} + 1)$$

Ahora sea $l > c$, supongamos que l no divide a a, luego entonces tomemos k'_a el entero positivo más pequeño que cumple $k'_a l > a$. Entonces, se tiene que:

$$q^a - 1 = (q^l - 1)(q^{a-l} + q^{a-2l} + ... + q^{a-(k'_a-2)l}) + (q^{a-(k-2)l} - 1)$$

Luego, $q^l - 1$ no divide a $q^a - 1$ para $l > mcd(a, b)$ y entonces quedaría probado el resultado. □

Gracias a este resultado, sabemos que la ecuación (4.8) y equivalentemente (4.7), tienen como máximo $q^{mcd(\theta,n)}$ soluciones. Por tanto, si a partir de R surgen t ecuaciones linealmente independientes, el conjunto de soluciones del sistema forma un subespacio vectorial de $\mathbb{F}_q^n$ de dimensión $n - t$, ya que cada solución de (4.7) es un subespacio de dimensión 1 linealmente independiente. Luego, el sistema tendrá q^{n-t} soluciones. Con esto se tiene que $q^{n-t} \leq q^{mcd(\theta,n)}$, que implica

$$n - t \leq mcd(\theta, n) \Longrightarrow n - mcd(\theta, n) \leq t$$

El siguiente teorema nos dará una cota para el número de soluciones.

Teorema 4.5 *Sean $\{f_1, ..., f_n\}$ las n componentes de F y sea $\mathcal{L}$ el espacio de linealización para F. Dado $\overline{z} = L_1^{-1}(\overline{y})$, si $\mathcal{L}_{\overline{z}}$ es el espacio de linealización que resulta de sustituir $\overline{z}$ en las ecuaciones de $\mathcal{L}$, entonces la dimensión de $\mathcal{L}_{\overline{z}}$ es al menos*

$$n - mcd(n, \theta) \geq \frac{2n}{3} \tag{4.9}$$

Salvo cuando $\overline{z} = (0, ..., 0)$ ya que en ese caso solo tenemos ecuaciones triviales.

Demostración: Estudiemos el valor de $mcd(\theta, n)$ en función de los valores que tome θ en MI. Como θ es estrictamente menor que n, el máximo valor que puede tomar $mcd(\theta, n)$ es $\frac{n}{2}$ y para ello debe darse que $\theta = \frac{n}{2}$. Si $\theta = \frac{n}{2}$, como $(q^n - 1) = (q^\theta + 1)(q^\theta - 1)$ se tiene que $mcd(q^n - 1, q^\theta + 1) = q^\theta + 1 > 1$. Esto contradice una de las condiciones de θ para MI. Por tanto, el valor máximo que podrá tomar $mcd(\theta, n)$ será $\frac{n}{3}$, siempre que 3 divida a n y $\theta = \frac{n}{3}$ o $\theta = \frac{2n}{3}$. Luego esto implica que $mcd(\theta, n) \leq \frac{n}{3}$ y entonces

$$n - mcd(\theta, n) \geq \frac{2n}{3} \tag{4.10}$$

□

Esto nos pone ya en situación de poder demostrar el teorema que nos dará la cota inferior para el número de ecuaciones de linealización linealmente independientes para las componentes de $\overline{F}$.

Teorema 4.6 *Sea $\overline{F} = \left\{\overline{f}_1, ..., \overline{f}_n\right\}$ las n componentes de la clave pública de un criptosistema MI y sea $\overline{\mathcal{L}}$ el espacio de linealización para $\overline{F}$. Dado $\overline{y} = (\overline{y}_1, ..., \overline{y}_n)$ un mensaje cifrado, si $\overline{\mathcal{L}}_{\overline{y}}$ es el espacio de linealización que resulta de sustituir $\overline{y}$ en las ecuaciones de $\overline{\mathcal{L}}$, entonces la dimensión de $\overline{\mathcal{L}}_{\overline{y}}$ es al menos*

$$n - mcd(n, \theta) \geq \frac{2n}{3} \tag{4.11}$$

Salvo en el caso $L_2^{-1}(\overline{y}) = (0, ..., 0)$ ya que en ese caso solo hay ecuaciones triviales.

La demostración de este teorema resulta de aplicar el Teorema 4.5 que nos daba una cota inferior para la dimensión de $\mathcal{L}_{\overline{z}}$ y el Lema 4.3 que relacionaba las dimensiones de $\mathcal{L}_{\overline{z}}$ y $\overline{\mathcal{L}_{\overline{y}}}$. Luego, sabemos que dado un criptosistema de Matsumoto e Imai, encontraremos como mínimo $\frac{2n}{3}$ ecuaciones de linealización linealmente independientes, lo cual reducirá enormemente la dificultad de obtener mensajes en claro conociendo únicamente la clave pública.

Para conocer exactamente la dimensión de $\overline{\mathcal{L}}$, debemos conocer cuantas ecuaciones linealmente independientes hay de la forma (4.1), sustituyendo para cada $i = 1, ..., n$ y_i por $\overline{f}_i(x_1, ..., x_n)$. Como hemos probado anteriormente la dimensión de $\overline{\mathcal{L}}$ es la misma que la de $\mathcal{L}$. Luego para probar este resultado buscaremos el número de ecuaciones linealmente independientes de la forma

$$\sum_{i=1}^{n}\sum_{j=1}^{n} a_{ij}x_i f_j(x_1, ..., x_n) + \sum_{i=1}^{n} b_i x_i + \sum_{j=1}^{m} c_j f_j(x_1, ..., x_n) + d = 0$$

donde $f_i(x_1, ..., x_n)$ son las componentes de la función F del esquema de MI.

Vamos a presentar el problema de las ecuaciones de linealización desde un punto de vista más genérico tal y como lo trabajan Diene et al. en [2]. Sea V un espacio vectorial, consideremos el conjunto $Fun(V, V)$ como el de las funciones de V en si mismo. Si $V = \mathbb{F}_q^n$, entonces $F \in Fun(V, V)$. Sean V y W dos espacios vectoriales cualesquiera, es trivial ver que el espacio de funciones de V en W, tiene estructura de espacio vectorial.

Definamos a continuación la aplicación $\psi_F : Fun(\mathbb{F}_q^n \times \mathbb{F}_q^n, \mathbb{F}_q) \longrightarrow Fun(\mathbb{F}_q^n, \mathbb{F}_q)$ de la siguiente manera:

$$\psi_F(g)(v) = g(v, F(v))$$

Dado que $Fun(V, W)$ es un espacio vectorial, tamhién lo será el conjunto de funciones $Fun(\mathbb{F}_q^n \times \mathbb{F}_q^n, \mathbb{F}_q)$. Ahora denotemos como $\mathcal{A}(\mathbb{F}_q^n)$ al conjunto de las aplicaciones afines de $\mathbb{F}_q^n$ en $\mathbb{F}_q$. Vamos a trabajar sobre el producto tensorial de este espacio consigo mismo, para darle estructura de espacio vectorial al conjunto sobre el que definiremos las ecuaciones de linealización. Ésto facilitará el cálculo de la dimensión de dicho espacio. Es claro ver que

existe una inmersión natural de $\mathcal{A}(\mathbb{F}_q^n) \otimes \mathcal{A}(\mathbb{F}_q^n)$ en $Fun(\mathbb{F}_q^n \times \mathbb{F}_q^n, \mathbb{F}_q)$, en la que conocidas $g, h \in \mathcal{A}(\mathbb{F}_q^n)$, y $x, x' \in \mathbb{F}_q^n$,

$$(g \otimes h)(x, x') = g(x)h(x')$$

Con esto, se puede definir un espacio de linealización de la aplicación $\overline{F}$ a través de la aplicación ψ_F restringida a $\mathcal{A}(\mathbb{F}_q^n) \otimes \mathcal{A}(\mathbb{F}_q^n)$. De manera más formal podemos escribirlo de la siguiente forma.

Definición 4.7 *Sea ψ_F la aplicación definida anteriormente, entonces el subespacio $\mathcal{L}_F = ker(\psi_F)|_{\mathcal{A}(\mathbb{F}_q^n)\otimes\mathcal{A}(\mathbb{F}_q^n)}$ se llama espacio de las ecuaciones de linealización sobre F.*

Definida la noción de ecuación de linealización de esta manera, nos encontramos con dos definiciones distintas para el espacio de linealización para un conjunto de polinomios dado. En el siguiente lema probaremos que son equivalentes.

Lema 4.8 *Las definiciones de espacio de linealización 4.1 y 4.7 son equivalentes.*

Demostración: Sea V^* el espacio dual de $\mathbb{F}_q^n$, recordemos que es el espacio de aplicaciones lineales de $\mathbb{F}_q^n$ en $\mathbb{F}_q$. Sea $\{g_i : i = 1, ...n\}$ una base de V^*, es claro que $\{g_i : i = 1, ...n\} \cup 1$ es una base de $\mathcal{A}(\mathbb{F}_q)$, luego por la Proposición 1.12 cualquier elemento de $\mathcal{A}(\mathbb{F}_q^n) \otimes \mathcal{A}(\mathbb{F}_q^n)$ será de la forma

$$\sum_{i=1}^{n}\sum_{j=1}^{n} a_{ij}(g_i \otimes g_j) + \sum_{i=1}^{n} b_i(g_i \otimes 1) + \sum_{j=1}^{n} c_j(1 \otimes g_j) + d(1 \otimes 1) \tag{4.12}$$

Ahora sea $x \in \mathbb{F}_q^n$, y sea $x_i = g_i(x)$ la i-ésima coordenada de x. Igualmente sea f_i una de las componentes de F, cada una de las coordenadas de $F(x)$ viene dada por $f_i(x) = g_i(F(x))$. Por la estructura del producto tensorial inmerso en $Fun(\mathbb{F}_q^n \times \mathbb{F}_q^n, \mathbb{F}_q)$ y por como está definida ψ_F, un elemento de $\mathcal{A}(\mathbb{F}_q^n) \otimes \mathcal{A}(\mathbb{F}_q^n)$ estará en $\mathcal{L}_F$ si, y solo si

$$\sum_{i=1}^{n}\sum_{j=1}^{n} a_{ij}x_i f_j(x) + \sum_{i=1}^{n} b_i x_i + \sum_{j=1}^{n} c_j f_j(x) + d = 0 \tag{4.13}$$

Luego, como hemos visto

$$\mu \in \mathcal{L}_F \iff \psi_F(\mu)(x) = 0$$

Y $\psi_F(\mu)(x) = 0$ es una ecuación de linealización definida como en la Definición 4.1. □

Para facilitar la demostración del resultado que nos interesa, levantaremos el problema del calculo de la dimensión del espacio de linealización en $\mathbb{F}_q$ a calcular la dimensión del espacio de linealización en $\mathbb{F}_{q^n}$.

Para simplificar los cálculos, en [2], a partir de la exactitud del tensor $\mathbb{F}_{q^n} \otimes -$ y propiedades de $Fun_{\mathbb{F}_q}(\mathbb{F}_{q^n} \times \mathbb{F}_{q^n}, \mathbb{F}_{q^n})$, se demuestra que la dimensión de $\mathcal{L}_F$ como $\mathbb{F}_q$-espacio vectorial coincide con la dimensión de otro $\mathbb{F}_q$-espacio vectorial en el que es más fácil trabajar. Concretamente, se define para cada $F \in Fun(\mathbb{F}_{q^n}, \mathbb{F}_{q^n})$ la aplicación $\hat{\psi}_F : Fun(\mathbb{F}_{q^n} \times \mathbb{F}_{q^n}, \mathbb{F}_{q^n}) \to Fun(\mathbb{F}_{q^n}, \mathbb{F}_{q^n})$ dada por $\hat{\psi}_F(f)(x) = f(x, F(x))$, denotando $\hat{\mathcal{L}}_F = ker(\hat{\psi}_F)|_{\mathbb{F}_{q^n}\otimes\mathcal{A}(\mathbb{F}_{q^n})\otimes\mathcal{A}(\mathbb{F}_{q^n})}$, se tiene que $\hat{\mathcal{L}}_F$ es isomorfo a $\mathbb{F}_{q^n} \otimes \mathcal{L}_F$ y, por tanto, $dim_{\mathbb{F}_q}(\mathcal{L}_F) = dim_{\mathbb{F}_{q^n}}(\hat{\mathcal{L}}_F)$. De esta

forma, se traslada al cálculo de elementos de $\mathbb{F}_{q^n} \otimes \mathcal{A}(\mathbb{F}_{q^n}) \otimes \mathcal{A}(\mathbb{F}_{q^n})$, cuya imagen por $\hat{\mathcal{L}}_F$ sea 0. Por otra parte, se tiene que $Fun_{\mathbb{F}_q}(\mathbb{F}_{q^n} \times \mathbb{F}_{q^n}, \mathbb{F}_{q^n})$ puede ser identificado como espacio vectorial con $\mathbb{F}_{q^n}(G \times G)$ (combinaciones lineales de producto de endomorfismos del grupo de Galois con coeficientes en $\mathbb{F}_{q^n}$) con G el grupo de Galois $Gal(\mathbb{F}_{q^n}, \mathbb{F}_q)$. Además, este último es finito y generado por X^q, entonces cada elemento de $Gal(\mathbb{F}_{q^n}, \mathbb{F}_q)$ vendrá dado por X^{q^i} con $i = 0, ..., n-1$. Luego, todo elemento de $\mathbb{F}_{q^n} \otimes \mathcal{A}(\mathbb{F}_{q^n}) \otimes \mathcal{A}(\mathbb{F}_{q^n})$ es de la forma

$$\sum_{i=0}^{n-1}\sum_{j=0}^{n-1} A_{ij} \otimes X^{q^i} \otimes X^{q^j} + \sum_{i=0}^{n-1} B_i \otimes X^{q^i} \otimes 1 + \sum_{j=0}^{n-1} C_j \otimes 1 \otimes X^{q^j} + D \otimes 1$$

En lo que sigue, debido a que estamos tratando un ataque para un criptosistema MI, consideraremos $q = 2^m$. La imagen del elemento anterior por $\hat{\psi}_F$ es:

$$\sum_{i=0}^{n-1}\sum_{j=0}^{n-1} A_{ij} X^{2^{mi}} (X^{2^{m\theta}+1})^{2^{mj}} + \sum_{i=0}^{n-1} B_i X^{2^{mi}} + \sum_{j=0}^{n-1} C_j (X^{2^{m\theta}+1})^{2^{mj}} + D \tag{4.14}$$

El objetivo será comprobar la dimensión de $\hat{\mathcal{L}}_F$. Como los elementos del núcleo tienen que hacer cero la ecuación anterior, entonces el término independiente deberá ser nulo, quedándonos elementos de la siguiente forma

$$\sum_{i=0}^{n-1}\sum_{j=0}^{n-1} A_{ij} \otimes X^{2^{mi}} \otimes X^{2^{mj}} + \sum_{i=0}^{n-1} B_i \otimes X^{2^{mi}} \otimes 1 + \sum_{j=0}^{n-1} C_j \otimes 1 \otimes X^{2^{mj}}$$

Enunciemos un lema que hará más sencillo el cálculo de la dimensión de $\tilde{\mathcal{L}}_F$.

Lema 4.9 *Sea* $\mathcal{M} = \left\{X^{2^{mi}} \otimes X^{2^{mj}}, X^{2^{mi}} \otimes 1, 1 \otimes X^{2^{mj}} : i, j = 0, ..., n-1\right\}$, *entonces*

$$dim(\hat{\mathcal{L}}_F) = n^2 + 2n - |\hat{\psi}_F(\mathcal{M})|$$

Demostración: Sea $\mathcal{N} = \left\{X^{2^{mi}} : i = 0, ..., n-1\right\}$, $\mathcal{N} \cup \{1\}$ es una base para $\mathbb{F}_{q^n} \otimes \mathcal{A}(\mathbb{F}_{q^n})$. Para comprobar esta afirmación, basta ver que $\mathbb{F}_{q^n} \otimes \mathcal{A}(\mathbb{F}_{q^n})$ y $\mathcal{A}(\mathbb{F}_{q^n})$ son isomorfos. Y vemos que es trivial comprobar que la aplicación

$$\begin{array}{rccc} \Phi: & \mathbb{F}_{q^n} \otimes \mathcal{A}(\mathbb{F}_{q^n}) & \longrightarrow & \mathcal{A}(\mathbb{F}_{q^n}) \\ & 1 \otimes X^{2^{mi}} & \longmapsto & X^{2^{mi}} \end{array}$$

es un isomorfismo. Esto unido a la Proposición 1.13, induce que $\mathcal{M} \cup \{1 \otimes 1\}$, claramente es una base para $\mathbb{F}_{q^n} \otimes \mathcal{A}(\mathbb{F}_{q^n}) \otimes \mathcal{A}(\mathbb{F}_{q^n})$. Entonces dado que $\hat{\psi}_F(1 \otimes 1) = 1$, se tiene que $\hat{\psi}_F(\mathcal{M}) \subseteq \mathcal{N}$. Luego

$$dim(im(\hat{\psi}_F)) = |\hat{\psi}_F(\mathcal{M} \cup \{1 \otimes 1\})| = |\hat{\psi}_F(\mathcal{M})| + 1$$

Esto y la fórmula de las dimensiones implica

$$\begin{aligned} dim(ker(\hat{\psi}_F)) =& dim(\mathbb{F}_{q^n} \otimes \mathcal{A}(\mathbb{F}_{q^n}) \otimes \mathcal{A}(\mathbb{F}_{q^n})) - dim(im(\hat{\psi}_F)) = \\ &= n^2 + n + n + 1 - (|\hat{\psi}_F(\mathcal{M})| + 1) = \\ &= n^2 + 2n - |\hat{\psi}_F(\mathcal{M})| \end{aligned}$$

□

Esto reduce la dificultad de calcular la dimensión del espacio de linealización al cálculo de $|\hat{\psi}_F(\mathcal{M})|$.

Como $\mathbb{F}_{q^n}$ es un cuerpo finito con cardinal 2^{mn}, por el Lema 1.4, $X^{2^{mn}} = X$. Por tanto, para facilitar el cálculo del cardinal de la imagen de $\hat{\psi}_F$, vamos a tomar los exponentes de la ecuación (4.14) con elementos de $\mathbb{Z}/(2^{mn}-1)\mathbb{Z}$.

Ahora construyamos una aplicación ϕ de la siguiente manera. Sean $\mathbb{Z}/n\mathbb{Z}^1$ y $\mathbb{Z}/n\mathbb{Z}^2$ dos copias de $\mathbb{Z}/n\mathbb{Z}$. $\phi : (\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}) \cup \mathbb{Z}/n\mathbb{Z}^1 \cup \mathbb{Z}/n\mathbb{Z}^2 \longrightarrow \mathbb{Z}/(2^{mn}-1)\mathbb{Z}$ se define de la siguiente manera

$$\phi(i,j) = 2^{mi} + 2^{mj} + 2^{m(\theta+j)} \quad si \quad (i,j) \in (\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z})$$

$$\phi(k) = 2^{mk} \quad si \quad k \in \mathbb{Z}/n\mathbb{Z}^1$$

$$\phi(l) = 2^{ml} + 2^{m(\theta+l)} \quad si \quad l \in \mathbb{Z}/n\mathbb{Z}^2$$

Claramente $|\hat{\psi}_F(\mathcal{M})| = |im(\phi)|$.

A continuación, escribiremos los términos de la imagen de ϕ en base 2^m. Es decir, si tenemos $n = 5$ el número correspondiente a la expresión 12010 es $2^{m\cdot 4} + 2 \cdot 2^{m\cdot 3} + 2^m$. Podemos representar el número con un diagrama circular en el que marcamos un vértice por cada dígito que tenga el número en base 2^m y etiquetamos cada vértice con el dígito correspondiente. Colocaremos en la parte superior del diagrama el dígito correspondiente a $2^{m(n-1)}$ e iremos colocando el resto en sentido horario. Véase un ejemplo de diagrama con el número anterior 12010.

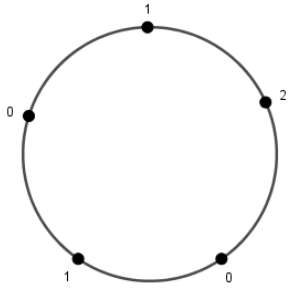


Figura 4.1: Diagrama representativo del número 12010 en base 2^m

Para completar la demostración vamos a ver los valores de $|im(\phi)|$ en función de los valores que tome θ.

Teorema 4.10 *Si $q = 2^m > 2$ entonces*

$$im(\phi) = \begin{cases} n^2 + \dfrac{4n}{3} & si \quad n = 3\theta, \dfrac{3\theta}{2} \\ \dfrac{n^2 + 3n}{2} & si \quad n = 2\theta \\ n^2 + n & en \quad otro \quad caso \end{cases}$$

Demostración: Para probar este resultado, consideremos la cantidad de diagramas distintos que tenemos en $im(\phi)$. Para ello, empezaremos a contar las posiciones en el diagrama de la siguiente forma, la posición 0 será la correspondiente al vértice superior, y contaremos siguiendo el orden de las agujas del reloj.

1. Dado $k \in \mathbb{Z}/n\mathbb{Z}^1$, $\phi(k)$ consistirá en un diagrama con un 1 en la posición k y el resto 0.

2. Dado $l \in \mathbb{Z}/n\mathbb{Z}^2$, $\phi(l)$ consistirá en un diagrama con dos 1, uno de ellos en la posición l y el otro en la posición $l + \theta$ luego tendremos dos 1 a distancia θ y el resto 0.

3. Dado $(i, j) \in \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, podemos distinguir dos casos:

   a) Cuando $i = j$ o $i = j + \theta$, $\phi(i, j)$ consistirá en un diagrama con un 2 en la posición i y un 1 en la posición $i + \theta$ en el primer caso y un 1 en la posición j en el segundo caso. Luego tendremos diagramas con un 2 y un 1 a distancia θ y el resto 0.

   b) En otro caso tendremos diagramas con tres 1 situados en las posiciones i, j y $j + \theta$, luego dos de ellos estarán a distancia θ, y el resto todo ceros.

Completaremos la prueba contando el número de diagramas que hay de cada tipo en función de los valores de θ. Hay n diagramas del primer tipo, uno para cada $k \in \mathbb{Z}_n^1$. En cuanto a los diagramas de tipo 2., habrá n siempre y cuando $n \neq 2\theta$ ya que en ese caso habrá $n/2$ distintos. Del tipo 3(a) hay $2n$ ya que tenemos n diagramas distintos cuando $i = j$ y otros tantos cuando $i = j + \theta$. Sin embargo, cuando $n = 2\theta$ habrá únicamente n diagramas de este tipo.

Por último, nos centraremos en los del tipo 3(b) ya que son los más complejos. Supongamos en primer lugar que $n \neq 2\theta$. En ese caso, comencemos considerando los diagramas que únicamente tienen dos 1 a distancia θ. Para el par de 1, tenemos n posiciones distintas y para el restante, tenemos todas aquellas menos en las que están situadas los dos primeros y aquellas posiciones que se encuentran a distancia θ de éstos. Por ello, tendremos $n - 4$ posiciones distintas para el tercer 1 a excepción del caso que $n = 3\theta \quad o \quad \frac{3\theta}{2}$, en el cual, para el tercer 1 tendremos $n - 3$ posiciones distintas en el diagrama. Cuando $n = 2\theta$, las posibilidades son más reducidas ya que tenemos $n/2$ posibles localizaciones para el primer par, y las $n - 2$ restantes para el tercero.

Cuando $n \neq 2\theta$ y $n \neq 3\theta, \frac{3\theta}{2}$, tenemos que contar también la posibilidad de que haya exactamente dos pares de 1 a distancia θ, dando lugar a n posibles diagramas. Y cuando

$n = 3\theta$ o $\frac{3\theta}{2}$ podemos tener $n/3$ posibles diagramas con los tres 1 a distancia θ.

Contados todos los diagramas posibles para los elementos de $im(\phi)$, solo nos queda agruparlos:

- Si $n = 3\theta$ o $n = \frac{3\theta}{2}$, $|im(\phi)| = n + n + 2n + n(n-3) + \frac{n}{3} = n^2 + \frac{4n}{3}$.
- Si $n = 2\theta$, $|im(\phi)| = n + \frac{n}{2} + n + \frac{n}{2}(n-2) = \frac{(n^2+3n)}{2}$.
- En cualquier otro caso, $|im(\phi)| = n + n + 2n + n(n-4) + n = n^2 + n$.

□

Cuando el cuerpo base es $\mathbb{F}_2$, es aún más delicado porque aparecen muchas otras condiciones que dificultan más el cálculo del cardinal de la imagen de ϕ.

Teorema 4.11 *Si $q = 2$, y $\theta = n/3$ o $\theta = 2n/3$, entonces*

$$im(\phi) = \begin{cases} 41 \quad si \quad n = 6, \ \theta = 2, 4 \\ 7 \quad si \quad n = 3, \ \theta = 1, 2 \\ n^2 + \dfrac{4n}{3} \quad en \quad otro \quad caso \end{cases}$$

Si $\theta = \frac{n}{2}$, entonces

$$im(\phi) = \begin{cases} 3 \quad si \quad n = 2, \\ \dfrac{n^2 + 3n}{2} \quad en \quad otro \quad caso \end{cases}$$

En otro caso,

$$im(\phi) = \begin{cases} 14 \quad si \quad n = 4, \ \theta = 1, 3 \\ n^2 \quad si \quad \theta = 1 \\ n^2 \quad si \quad n = 2\theta \pm 1, \ \theta + 1 \quad y \quad \theta > 1 \\ n^2 + \dfrac{n}{2} \quad si \quad n = 2\theta \pm 2 \\ n^2 + n \quad en \quad otro \quad caso \end{cases}$$

Demostración: Al igual que hicimos para el teorema anterior, la prueba consistirá en contar el número de diagramas distintos que hay en función de los valores de θ. En este caso, por darse la particularidad de darse que $m = 1$, los diagramas presentarán peculiaridades diferentes que no vimos en los diagramas del caso $q > 2$.

1. Dado $k \in \mathbb{Z}/n\mathbb{Z}^1$, $\phi(k)$ consistirá en un diagrama con un 1 en la posición k y el resto 0.

2. Dado $l \in \mathbb{Z}/n\mathbb{Z}^2$, $\phi(l)$ consistirá en un diagrama con dos 1, uno de ellos en la posición l y el otro en la posición $l + \theta$ luego tendremos dos 1 a distancia θ y el resto 0.

3. Dados $(i, j) \in (\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z})$, distinguiremos tres tipos:

a) Sea $i = j$, $\phi(i,i) = 2^{i+1} + 2^{\theta+1}$, luego en esta situación $im(\phi)$ consistirá en diagramas con dos 1 situados a distancia $\theta - 1$ y el resto 0.

b) Sea $j = \theta + 1$, luego $\phi(i,j) = 2^i + 2^{j+1}$, por tanto, en este caso $im(\phi)$ se trata de diagramas con dos 1 a distancia $\theta + 1$ y el resto todo 0.

c) En cualquier otro caso, tendremos diagramas con tres 1 situados en las posiciones i, j y $j + \theta$, luego dos de ellos estarán a distancia θ y el resto serán todo ceros.

Una vez descritos los distintos tipos de diagramas, solo tendremos que realizar un argumento de conteo idéntico al realizado en el Teorema 4.10, para concluir con la demostración del teorema. □

Ya desarrollados los dos teoremas anteriores, disponemos de todas las herramientas necesarias para enunciar el teorema de la dimensión del espacio de linealización para el criptosistema de Matsumoto e Imai como en [2]. (Nótese que para MI no se puede dar el caso $\theta = \frac{n}{2}$, por lo que no lo incluiremos en el enunciado del teorema),

Teorema 4.12 *(Teorema de la dimensión del espacio de linealización) Sea $\overline{F}$ la clave pública de un criptosistema MI, y sea $\overline{\mathcal{L}}$ el espacio de linealización de las componentes de $\overline{F}$. Entonces la dimensión exacta de $\overline{\mathcal{L}}$ en función de los parámetros de MI será la siguiente:*

Si $q > 2$, entonces

$$dim(\overline{\mathcal{L}}) = \begin{cases} \dfrac{2n}{3} & si \quad \theta = \dfrac{2n}{3}, \dfrac{n}{3} \\ n & en \quad otro \quad caso \end{cases}$$

Si $q = 2$ y $\theta = \frac{2n}{3}$ o $\theta = \frac{n}{3}$, entonces

$$dim(\overline{\mathcal{L}}) = \begin{cases} 7 & si \quad n = 6,\ \theta = 2,\ 4 \\ 8 & si \quad n = 3,\ \theta = 1,\ 2 \\ \dfrac{n^2 + 3n}{2} & en \quad otro \quad caso \end{cases}$$

Si $q = 2$ y $\theta \neq \frac{2n}{3}$ y $\theta \neq \frac{n}{3}$, entonces:

$$dim(\overline{\mathcal{L}}) = \begin{cases} 10 & si \quad n = 4,\ \theta = 1,\ 3 \\ 2n & si \quad \theta = 1,\ n-1,\ \dfrac{n \pm 1}{2} \\ \dfrac{3n}{2} & si \quad \theta = \dfrac{n}{2} \pm 1 \\ n & en \quad otro \quad caso \end{cases}$$

Demostración: Consideremos en primer lugar los Teoremas 4.10 y 4.11 que nos dan $|im(\phi)|$ en función de n, θ y q. Y luego, a partir del Lema 4.8, calcularemos $dim(\tilde{\mathcal{L}_F}) = n^2 + 2n - |\tilde{\psi}_F(\mathcal{M})|$ previa identificación $|im(\phi)| = |\tilde{\psi}_F(\mathcal{M})|$. Realizando esta operación en función de cada uno de los valores posibles para n, θ y q, y aplicando el Lema 4.3, concluimos con cada uno de los valores posibles para $dim(\overline{\mathcal{L}})$. □

4.2. Construcción de las ecuaciones de linealización

Hemos hablado a lo largo del capítulo únicamente sobre la dimensión del espacio de linealización, y todavía no sabemos como construir las ecuaciones conociendo únicamente la clave pública. Ya que Patarin da una primera construcción del espacio de linealización para $\tilde{F}$ pero sucede que en los criptosistemas MI el valor de θ no siempre es público, luego nos encontraremos situaciones en las que no conozcamos $\tilde{F}$. Por lo que en esta sección explicaremos como generar realmente ecuaciones de linealización. Para ello se pueden emplear dos métodos distintos.

Textos en claro-textos cifrados

Como el conocimiento de la clave pública permite cifrar mensajes en claro, entonces mediante pares $y' = \overline{F}(x')$ se generan ecuaciones de la forma

$$\sum_{i=1}^{n}\sum_{j=1}^{m} a_{ij}x'_i y'_j + \sum_{i=1}^{n} b_i x'_i + \sum_{j=1}^{m} c_j y'_j + d = 0 \tag{4.15}$$

en las variables a_{ij},b_i,c_j y d. Luego por cada mensaje en claro y su correspondiente cifra se genera una ecuación en $n^2 + n + n + 1 = (n+1)^2$ variables. Por tanto, escogiendo $(n+1)^2$ pares de mensajes en claro y cifrado podemos obtener suficientes ecuaciones de la forma (4.15) y obtener las ecuaciones correspondientes para el desarrollo del ataque. Esto conllevará cifrar $(n+1)^2$ mensajes y más adelante resolver un sistema de $(n+1)^2$ ecuaciones en $(n+1)^2$ variables. Luego computacionalmente el ataque construyendo ecuaciones con este método parece viable. Dependerá únicamente de la suerte que tengamos al escoger los mensajes, ya que las ecuaciones resultantes pueden ser o no linealmente independientes.

Estructura polinomial de $\overline{F}$

Como sabemos en un criptosistema MI, la función de cifrado $\overline{F}$ está formada por n componentes polinomiales de grado 2. Dados $\overline{f}_i$ las componentes de $\overline{F}$, y sea una ecuación de linealización del tipo (4.1). Si sustituimos los polinomios correspondientes a cada $\overline{f}_j$ por y_j nos queda una ecuación de grado 3 del tipo

$$\sum_{i=1}^{n}\sum_{j=1}^{n}\sum_{k=1}^{n} \alpha_{ijk}x_i x_j x_k + \sum_{i=1}^{n}\sum_{j=1}^{n} \beta_{ij}x_i x_j + \sum_{i=1}^{n} \gamma_i x_i + \delta = 0 \tag{4.16}$$

Donde cada uno de los α_{ijk}, β_{ij}, γ_i y δ representan combinaciones lineales de los elementos a_{ij}, b_i, c_j y d de la ecuación (4.1). Para que estas ecuaciones se anulen en todos los valores de $x \in \mathbb{F}_q^n$, dichos coeficientes deben de ser 0. Esto implica, que para "el desarrollo del ataque"debemos resolver un sistema de $\frac{(n+1)(n+2)(n+3)}{6}$ ecuaciones en $(n+1)^2$ variables. Veamos de donde sale este número.

Tenemos una ecuación para cada uno de los coeficientes de (4.16), luego tenemos que saber cuantos coeficientes hay.

- Términos de grado tres:
  - x_i^3: hay un término para cada i, luego n coeficientes.
  - $x_i^2 x_j$: hay $n(n-1)$ términos.
  - $x_i x_j x_k$: hay $\binom{n}{3}$ términos.
- Términos de grado dos:
  - x_i^2: hay un término para cada i, luego n coeficientes.
  - $x_i x_j$: en este caso hay $\binom{n}{2}$ términos.
- Términos de grado uno: hay únicamente n términos de grado uno, por tanto, n coeficientes.
- Por último un término de grado cero: δ

Luego si sumamos la cantidad de términos que hay en la ecuación anterior, tendremos:

$$n + n(n-1) + \binom{n}{3} + n + \binom{n}{2} + n + 1 = \frac{n^3 + 6n^2 + 11n + 6}{6} = \frac{(n+1)(n+2)(n+3)}{6}$$

Por tanto, para hacer posible el ataque debemos resolver un sistema de $\frac{(n+1)(n+2)(n+3)}{6}$ ecuaciones con $(n+1)^2$ incógnitas. Para conocer el espacio de linealización, solo nos resultaría necesario tomar $(n+1)^2$ de esas ecuaciones, que se espera que sean independientes, y comprobar que también satisfacen las restantes ya que si no será necesario tomar más ecuaciones. Por tanto, computacionalmente construir las ecuaciones de linealización por ambos métodos son parecidos. Luego a priori, podemos afirmar que este ataque es viable, dada las cotas para la dimensión del espacio de linealización y la construcción del mismo.

4.3. Ejemplo de un ataque por linealización

Si en el capítulo 3 construimos un criptosistema MI, ahora vamos a criptoanalizarlo a partir de ecuaciones de linealización para $\overline{F}$. Recordemos como estaba definida $\overline{F}$. Recordar que este es un ejemplo pequeño, tomando parámetros pequeños para hacer visible de una forma más sencilla como funcionan este tipo de ataques.

Dado $x = (x_1, x_2, x_3) \in \mathbb{F}_4^3$:

$$\begin{cases} \overline{f}_1(x_1, x_2, x_3) = \alpha x_1^2 + \alpha x_2^2 + (\alpha+1)x_1x_2 + \alpha x_2x_3 + (\alpha+1)x_2 + \alpha \\ \overline{f}_2(x_1, x_2, x_3) = (\alpha+1)x_2^2 + \alpha x_1x_2 + \alpha x_1x_3 + \alpha x_2x_3 + \alpha x_2 + \alpha x_3 \\ \overline{f}_3(x_1, x_2, x_3) = x_1^2 + x_2^2 + x_3^2 + x_1x_2 + \alpha x_2x_3 + x_2 \end{cases}$$

Donde tenemos que $n = 3$ y $\theta = 1 = \frac{n}{3}$. Por el teorema de las dimensiones, vemos que la dimensión del espacio de linealización para $\{\overline{f}_1, \overline{f}_2, \overline{f}_3\}$ debe ser 2. Hagamos los cálculos correspondientes para ver que eso es así.

De los dos métodos descritos anteriormente para construir ecuaciones de linealización utilizaremos el segundo, es decir, en las ecuaciones:

$$\sum_{i=1}^{3}\sum_{j=1}^{3} a_{ij}x_i\overline{f}_j(x_1,...,x_n) + \sum_{i=1}^{3} b_i x_i + \sum_{j=1}^{3} c_j\overline{f}_j(x_1,...,x_n) + d = 0$$

Sustituiremos $\overline{f}_j$ por sus expresiones explícitas, y tendremos una ecuación como la descrita en (4.16) para $n = 3$. Tendremos una ecuación de 20 términos, con sus respectivos coeficientes. Cada uno de los coeficientes es una combinación lineal de a_{ij}, b_i, c_j y d. Para que la ecuación sea idénticamente nula, cada uno de los 20 coeficientes deberá ser cero, esto nos llevará a un sistema de 20 ecuaciones y 16 incógnitas donde las incógnitas son a_{ij}, b_i, c_j y d. Como tenemos más ecuaciones que incógnitas podría parecer que no tiene solución, pero como ya hemos visto que por el teorema la dimensión tiene que ser 2, algunas de éstas serán dependientes.

Para facilitar los cálculos vamos a utilizar la siguiente notación: $d = A_0$, $c_j = A_j$ para $j = 1, 2, 3$, $b_i = A_{4i}$ para $i = 1, 2, 3$ y $a_{ij} = A_{4i+j}$ para $i, j = 1, 2, 3$. El siguiente paso, será resolver el sistema para obtener el espacio de linealización correspondiente a $\overline{f}_1$, $\overline{f}_2$ y $\overline{f}_3$. Éste vendrá dado por las siguientes ecuaciones.

$$\begin{aligned}
&A_0 + \alpha A_1 = 0\\
&A_4 + \alpha A_5 = 0\\
&(\alpha+1)A_1 + \alpha A_2 + A_3 + A_8 + \alpha A_9 = 0\\
&\alpha A_1 + A_3 = 0\\
&\alpha A_2 + A_{12} + \alpha A_{13} = 0\\
&\alpha A_1 + (\alpha+1)A_2 + A_3 + (\alpha+1)A_9 + \alpha A_{10} + A_{11} = 0\\
&A_3 + \alpha A_{14} = 0\\
&(\alpha+1)A_1 + \alpha A_2 + A_3 + (\alpha+1)A_5 + \alpha A_6 + A_7 = 0\\
&\alpha A_2 + \alpha A_6 = 0\\
&\alpha A_1 + \alpha A_2 + \alpha A_3 + (\alpha+1)A_{13} + \alpha A_{14} + A_{15} = 0\\
&(\alpha+1)A_5 + \alpha A_6 + A_7 + \alpha A_9 + A_{11} = 0\\
&\alpha A_6 + \alpha A_{13} + A_{15} = 0\\
&\alpha A_5 + (\alpha+1)A_6 + A_7 + (\alpha+1)A_9 + \alpha A_{10} + A_{11} = 0\\
&\alpha A_9 + \alpha A_{10} + \alpha A_{11} + \alpha A_{13} + (\alpha+1)A_{14} + A_{15} = 0\\
&A_7 + \alpha A_{14} = 0\\
&A_{11} + \alpha A_{13} + \alpha A_{14} + \alpha A_{15} = 0\\
&\alpha A_5 + A_7 = 0\\
&\alpha A_9 + (\alpha+1)A_{10} + A_{11} = 0\\
&A_{15} = 0\\
&\alpha A_5 + \alpha A_6 + \alpha A_7 + \alpha A_{10} + (\alpha+1)A_{13} + \alpha A_{14} + A_{15} = 0
\end{aligned}$$

Como ya sabemos a partir del teorema anterior, la dimensión del espacio de linealización va a ser 2, luego la solución a este sistema de ecuaciones nos dará un subespacio vectorial de

dimensión 2 sobre $\mathbb{F}_{2^2}$. Realizando los cálculos necesarios, obtenemos la siguiente solución en función de dos parámetros que serán A_2 y A_3.

$$\begin{aligned}
&A_0 = A_4 = A_7 = A_9 = A_3\\
&A_6 = A_{13} = A_2\\
&A_1 = A_5 = A_{14} = (\alpha+1)A_3\\
&A_8 = A_{11} = A_3 + \alpha A_2\\
&A_{10} = A_3 + (\alpha+1)A_2\\
&A_{12} = A_{15} = 0
\end{aligned}$$

Luego a partir de los parámetros podemos generar dos ecuaciones de linealización linealmente independientes. Sea (A_3, A_2) el vector de parámetros, y sean $(1,0)$, $(0,1)$ dos vectores de parámetros linealmente independientes, entonces las dos ecuaciones de linealización generadas a partir de ambos vectores son las siguientes

$$\begin{aligned}
&(\alpha+1)x_1y_1 + x_1y_3 + x_2y_1 + x_2y_2 + x_2y_3 + (\alpha+1)x_3y_2 + x_1 + x_2 + (\alpha+1)y_1 + y_3 + 1 = 0\\
&x_1y_2 + (\alpha+1)x_2y_2 + \alpha x_2y_3 + x_3y_1 + \alpha x_2 + y_2 = 0
\end{aligned} \tag{4.17}$$

Conocidas las ecuaciones, sea ahora $\overline{y} = (0, 1, \alpha+1)$ un mensaje cifrado, si sustituimos $\overline{y}$ por y en (4.17) nos quedará un sistema de ecuaciones en x_1, x_2, x_3, cuya solución contendrá al mensaje en claro. El sistema que resulta al sustituir $(0, 1, \alpha+1)$ por y está formado por estas dos ecuaciones

$$\begin{aligned}
&\alpha x_1 + (\alpha+1)x_2 + (\alpha+1)x_3 + \alpha = 0\\
&x_1 + 1 = 0
\end{aligned}$$

El conjunto de soluciones del sistema es el siguiente.

$$\begin{cases} x_1 = 1 \\ x_2 = x_3 \end{cases} \Longrightarrow \begin{cases} (1,0,0) \\ (1,1,1) \\ (1,\alpha,\alpha) \\ (1,\alpha+1,\alpha+1) \end{cases}$$

Esto nos da un conjunto de cuatro elementos entre el que se encuentra el mensaje en claro. De entre esos cuatro elementos podemos obtener el mensaje de dos formas, una cifrando todos los mensajes y viendo cual produce $\overline{y}$. Y otra sustituyendo la solución del sistema que resulta de sustituir (x_1, x_2, x_3) por $(1, x_3, x_3)$ en la función de cifrado y resolviendo tres ecuaciones en la incógnita x_3, lo cual convierte al problema de descifrar mensajes únicamente a partir de la clave pública en un problema viable.

Si aplicamos el primer método y ciframos todos los mensajes vemos que la solución correcta es $(1,1,1)$, veáse como

$$\overline{F}(1,1,1) = (\overline{f}_1(1,1,1), \overline{f}_2(1,1,1), \overline{f}_3(1,1,1)) = (0, 1, \alpha+1)$$

Y si empleamos el segundo método descrito anteriormente nos queda un sistema de ecuaciones de la siguiente forma

$$\begin{cases} 0 = 0 \\ x_3^2 = 1 \\ \alpha x_3^2 + 1 = \alpha + 1 \end{cases}$$

Y resolviendo nos queda la solución ya conocida $\overline{x} = (1, 1, 1)$. Luego a partir de un mensaje cifrado, y conociendo únicamente la clave pública hemos obtenido el mensaje en claro correspondiente. A partir de las ecuaciones de linealización (4.17), podemos introducir cualquier mensaje cifrado por $\overline{F}$ que obtendremos el mensaje en claro con un sencillo cálculo. Esto vulnera la seguridad de nuestro criptosistema.

Bibliografía

[1] AKKAR, M-L., COURTOIS, N., DUTUEIL, R., y GOUBIN, L.,*A fast and secure implementation of Sflash.* En Desmedt, Y.G., editor. *Public Key Cryptography - PKC 2003: 6th International Workshop on Practice and Theory in Public Key Cryptography*, Miami, FL, USA, volumen 2567 de LNCS, 267-278. Springer. (2003).

[2] DIENE, A., DING, J., GOWER, J., HODGES, T., y YIN, Z., *Dimension of The Linearization Equations of the Matsumoto-Imai Cryptosystems.* En Ytrheus, O., editor, *The International Workshop on Coding and Cryptography* (WCC 2005), Bergen, Norway, volumen 3969 de Lecture Notes in Computer Science, 242-251. Springer. (2006).

[3] DIFFIE, W., y HELLMAN, M., *New directions in cryptography.* Transactions on Information Theory, 644-654. (1976).

[4] DING, J., GOWER, J. y SCHMIDT, D., *Multivariate Public Key Cryptosystems.* University of Cincinnati, USA, Springer, (2006).

[5] FELL, H., Y DIFFIE, W., . *Analysis of a public key approach based on polynomial substitution.* Advances in cryptology—CRYPTO '85, volumen 218 de LNCS, 340-349. Springer. (1986).

[6] FERNANDEZ-FERREIROS, P., *Teoría de Galois.* Universidad de Cantabria. (2017)

[7] GILES, M., *¿Qué es la criptografía poscuántica y por qué se volverá impresdincible?* (Traducido al español por Ana Milutinovic), MIT Techhnology Review, [en línea], (2009). Disponible en: `https://www.technologyreview.es/s/11310/que-es-la-criptografia-poscuantica-y-por-que-se-volvera-impresdincible`. [Fecha de consulta: 12 de agosto de 2020].

[8] KIPNIS, A., y SHAMIR, A., *Cryptanalysis of the HFE Public Key Cryptosystem*,En Wiener, M., editor, *Advances in Cryptology - CRYPTO 1999*, volumen 1666 of LNCS, 19-30. Michael Wiener, Springer, (1999).

[9] LANG, S., *Algebra*, Revised Third Edition. Springer. (2002).

[10] LEZAMA, O., *Producto tensorial de espacios vectoriales y matrices*, En *Algebra Lineal*, Capítulo 11, sección 4. Universidad Nacional de Colombia. [en línea]. Disponible en: `http://red.unal.edu.co/cursos/ciencias/2001004/lecciones/cap11/cap11s4.pdf`. [Fecha de consulta: 3 de agosto de 2020].

[11] MATSUMOTO, T., y IMAI, H., *Public quadratic polynomial-tuples for efficient signature verification and message encryption.*, Advances in cryptology - EUROCRYPT '88, volume 330 of LNCS, 419-453. Springer. (1988).

[12] ONG, H., SCHNORR, C. y SHAMIR, A., *Efficient signatures schemes based on polynomial equations.* En Blakley, G. R. y Chaum, D., editores, *Advances in cryptology, Crypto '84*, volumen 196 de LNCS, 37-46. Springer. (1985).

[13] PATARIN, J., *Asymmetric cryptography with a hidden monomial.* En Koblitz, N., editor. *Advances in cryptology, CRYPTO '96*, volumen 1109 de LNCS, 45-60. Springer. (1996).

[14] PATARIN, J., *Cryptanalysis of the Matsumoto and Imai Public Key Scheme of Eurocrypt'98*, Designs, Codes and Cryptography, 20, 175–209. Kluwer Academic Publishers, Boston. (2000).

[15] POLLARD, J. y SCHNORR, C., *An efficient solution for the congruence* $x^2 + ky^2 = m$ *(mod* n*)*. IEEE Trans Inform. Theory, 33(5), 702-709. (1987).

[16] RIVEST, R.L., SHAMIR, A., y ADLEMAN, L.M., *Method for obtaining digital signatures and public key cryptosystems. secure communications and asymmetric cryptosystems.* En Simmons, G, editor, AAAS Sels, volumen 69, 217-239. Westview Press. (1978).

[17] RUIZ, C., *Ampliación de Matemáticas, Clasificación de Grupos Finitos*, [en línea]. Departamento de Matemáticas, Universidad Complutense de Madrid. Disponible en: `http://www.mat.ucm.es/~cruizb/2-AM/Apuntes-i/Apuntes-14/Grupos-10.pdf`. [Fecha de consulta: 2 de junio de 2020].

[18] SULLIVAN, N., *A (Relatively Easy To Understand) Primer on Elliptic Curve Cryptography*, [en línea] The Cloudflare Blog. (2013). Disponible en: `https://blog.cloudflare.com/a-relatively-easy-to-understand-primer-on-elliptic-curve-cryptography/`. [Fecha de Consulta: 24 de agosto de 2020].

[19] WOLF, C. y PRENEEL, B., *Taxonomy of Public Key Schemes based on the problem of Multivariate Quadratic equations.* ESAT-COSIC, Cryptology ePrint Archive, Report 2005/077, (2005).