# Introducción a Criptografía Multivariable

Miguel Esteban Pérez Ibarra

19 de octubre de 2020

## 1. Introducción a Polinomios

**Definicón 1.1**.(Anillo de polinomios $F[x]$). Sea $F$ un campo. Le llamaremos el anillo de polinomios sobre $F$ en la indeterminada $x$, al conjunto representado por $F[x]$, cuyos elementos son de la forma:

$$a_0 + a_1x + ... + a_nx^n.$$

Aquí $n$ puede ser cualquier entero no negativo y donde los coeficientes $a_0, a_1, ..., a_n \in F$.

**Ejemplo 1.1.1**. Consideré el campo $\mathbb{Z}_2 = \{\bar{0}, \bar{1}\}$. Entonces se cumple que

$$\mathbb{Z}_2[x] = \{a_0 + a_1x + a_2x^2 + \cdots + a_nx^n : a_i \in \mathbb{Z}_2\}$$

es un anillo de polinomios en el campo $\mathbb{Z}_2$ y un polinomio en particular de $p(x) \in \mathbb{Z}_2[x]$ sería

$$p(x) = \bar{1} + \bar{0}x + \bar{1}x^2.$$

**Definición 1.2**. Sean $p(x) = a_0 + a_1x + ... + a_mx^m$ y $q(x) = b_0 + b_1x + ... + b_nx^n$ entonces la suma y el producto se definen de la sigiente forma:

1. $p(x) + q(x) = c_1x + ... + c_mx^t$ donde $c_i = a_i + b_i \ \ \forall i$.
2. $p(x)q(x) = d_1x + ... + d_kx^k$ donde $d_t = a_tb_0 + a_{t-1}b_1 + a_{t-2}b_2 + ... + a_0b_t$

**Definición 1.2.1**. Si $f(x) = a_0 + a_1x + ... + a_nx^n \neq 0$ y $a_n \neq 0$, entonces el grado de $f(x)$, escrito como $\deg f(x)$, es $n$.

**Ejemplo 1.2.2**. Sean $p(x), q(x) \in \mathbb{Z}_2[x]$. tales que $p(x) = \bar{1} + x^2$ y $q(x) = \bar{1} + x$, entonces:

$$p(x) + q(x) = (\bar{1} + x^2) + (\bar{1} + x) = \bar{2} + x + x^2 = x + x^2.$$
$$p(x)q(x) = (\bar{1} + x^2)(\bar{1} + x) = \bar{1} + x + x^2 + x^3 = \bar{1} + x + x^2 + x^3.$$

**Teorema 1.3**. Dados dos polinomios $f(x)$ y $g(x)$ de $F[x]$ con $g(x) \neq 0$, existen entonces dos polinomios $t(x)$ y $r(x)$ en $F[x]$ tales que $f(x) = t(x)g(x) + r(x)$ donde $r(x) = 0$ o $\deg(r) < \deg(g)$.

**1.3.1**. Ejemplo con $f(x)$, $g(x) \in F[x]$.

**Definición 1.4**. Un subconjunto $I \subset R$ se llama ideal si se cumplen las siguientes condiciones $\forall x, y \in I$:

1. $x - y \in I$.
2. $xr, rx \in I$, $\forall r \in R$

**Ejemplo 1.4.1**. Considere el anillo de los enteros $\mathbb{Z}$. Si suponemos que $I = \{nk : k \in \mathbb{Z}\}$, note que dados $a, b \in \mathbb{Z}$ existen $k_1, k_2 \in \mathbb{Z}$ tales que $a = nk_1$ y $b = nk_2$. Luego se cumple que $a+b = n(k_1+k_2)$ y $ar = n(k_1 r)$, por tanto ambos $a + b, ar \in I$ con $r \in \mathbb{Z}$ arbitrario.

**Proposición 1.4.2**. Sea $R$ un anillo conmutativo y sea $a \in R$. El conjunto $\{ar : r \in R\}$ de todos los multiplos de $a$ en un ideal de $R$ se llama el **ideal principal** generado por $a$. Denotamos pues $(a) = \{ar : r \in R\}$.

**Ejemplo 1.4.3**. Dado que por lo mientras nos interesan los polinomios, basado en la proposición anterior considerese el siguiente ejemplo: sea $\mathbb{Q}[x]$ el conjunto de los polinomios con entrada en los racionales. Enfoquemonos en el polinomio $f(x) = x^2 - 2$ en $\mathbb{Q}[x]$, entonces se cumple que $f(x)$ es factor para cada $g(x)$ en:

$$(x_2 - 2) = \{(x_2 - 2)p(x) : p(x) \in \mathbb{R}[x]\}$$

También podemos considerar al ideal principal:

$$(x) = xp(x) : p(x) \in \mathbb{R}[x]$$

Este ideal se puede ver como el conjunto de todos los polinomios que tiene como raíz al cero.

**Proposición y Definición 1.5**. Sea $R$ un anillo y consideré $I \subset R$ un ideal. Se cumple que $R/I = \{I + r : r \in R\}$ es un anillo bajo las operaciones binarias:

$$(I + r) + (I + s) = I + (r + s) \text{ y } (I + r)(I + s) = I + (rs).$$

para cualesquiera $r, s \in R$. Cuando $I$ sea un ideal del anillo $R/I$ con las operaciones anteriores se llama el anillo cociente de $R$ sobre $I$.

**Ejemplo 1.5.1**. Considere al anillo $\mathbb{Z}_6$, por definición tenemos que $I = \{\bar{0}, \bar{2}, \bar{4}\}$ en un ideal generado por $(\bar{2})$ en $\mathbb{Z}_6$. Ahora si queremos estudiar la forma de $\mathbb{Z}_6/I$, sabemos que $R/I = \{I + r : r \in R\}$ por lo anterior. Entonces tenemos la siguiente igualdad:

$$\mathbb{Z}_6/I = \{I + \bar{i} : \forall i = \bar{1}, ..., \bar{5}\}$$

Sin embargo dado que se opera en $\mathbb{Z}_6$ se obtiene que $I = I + \bar{0} = I + \bar{2} = I + \bar{4}$ y además $I = I + \bar{1} = I + \bar{3} = I + \bar{5}$. Por tanto queda claro que:

$$\mathbb{Z}_6/I = \{I, I + \bar{1}\}$$

**Proposición 1.6**. $f(x) \equiv g(x) \mod (p(x))$ ssi $f(x)$ y $g(x)$ tienen el mismo residuo al dividirse por $p(x)$.

**Teorema 1.7**. (Caracterización de $F[x]/P$). Si $F$ es un campo, sea $P$ el ideal $(p(x))$ en $F[x]$ generado por el polinomio $p(x)$ de grado $n > 0$. Los elementos de $F[x]/P$ son de la forma:

$$P + a_0 + a_1x + \cdots + a_{n-1}x^{n-1} \text{ donde } a_0, a_1, \cdots, a_{n-1} \in F.$$

**Ejemplo 1.7.1**. Sea $P = (x^2 + x + \bar{1})$ en $\mathbb{Z}_2[x]$ generado por $p(x) = x^2 + x + \bar{1}$. Por el teorma de arriba se cumple que $P + x$ y $P + x + \bar{1} \in \mathbb{Z}_2[x]/P$, ya que $\bar{0}$ y $\bar{1} \in \mathbb{Z}_2$. Es decir:

$$\mathbb{Z}_2/(x^2 + x + 1) = \{P + a_1x + a_0 : a_0, a_1 \in \mathbb{Z}_2\} = \{P, P + 1, P + x + 1\}.$$

**Tabulación 1.7.2**. Entonces la suma y multiplicación de estos dos se encuentran como sigue:

$$(P + x) + (P + x + \bar{1}) = P + (x + (x + \bar{1})) = P + (\bar{2}x + \bar{1}) = P + \bar{0}x + \bar{1} = P + \bar{1}.$$
$$(P + x)(P + x + \bar{1}) = P + (x(x + 1)) =$$
$$P + (x^2 + x) = P + (x^2 + x + 0) = P + (x^2 + x + 1) + 1 = P + 1.$$

Análogamente se procede con los demas elementos de $\mathbb{Z}_2/(x^2 + x + 1)$ para así formar una tabla:

Ring $\mathbb{Z}_2/(x^2 + x + 1)$

| $+$ | $P$ | $P+1$ | $P+x$ | $P+x+1$ |
|---|---|---|---|---|
| $P$ | $P$ | $P+1$ | $P+x$ | $P+x+1$ |
| $P+1$ | $P+1$ | $P$ | $P+x+1$ | $P+x$ |
| $P+x$ | $P+x$ | $P+x+1$ | $P$ | $P+1$ |
| $P+x+1$ | $P+x+1$ | $P+x$ | $P+1$ | $P$ |

| $\cdot$ | $P$ | $P+1$ | $P+x$ | $P+x+1$ |
|---|---|---|---|---|
| $P$ | $P$ | $P$ | $P$ | $P$ |
| $P+1$ | $P$ | $P+1$ | $P+x$ | $P+x+1$ |
| $P+x$ | $P$ | $P+x$ | $P+x+1$ | $P+1$ |
| $P+x+1$ | $P$ | $P+x+1$ | $P+1$ | $P+x$ |

**Teorema 1.7.3**. Sea $a \in R$ donde $R$ es un anillo euclideano. Se cumple que cociente $R/(a)$ es un campo si, y solamente si $a$ es irreducible en $R$.

**Corolario 1.7.3**. $\mathbb{Z}_p = \mathbb{Z}/(p)$ es un campo si, y solo si $p$ es primo.

**Teorema 1.8**. El anillo $F[x]/(p(x))$ es un campo si, y solo si $p(x)$ es irreducible sobre un campo $F$.

**Ejemplo 1.8.1**. El polinomio $p(x) = \bar{1} + x + x^2$ es irreducible en el campo $\mathbb{Z}_2$.

**Ejemplo 1.9**. Se obtine que $\mathbb{Z}_2[x]/(p(x))$ con $P(x) = \bar{1} + x + x^2$ es un campo ya que como vimos arriba $p(x)$ es irreducible sobre el campo $\mathbb{Z}_2$.

**1.10**. La característica de un anillo $R$ se define como el entero positivo más pequeño $n$ en donde

$$\sum_{i=1}^{n} 1_R = 0.$$

Si no existe tal $n$, decimos que la característica de $R$ es 0. Ahora, para un campo $F$ se cunple que la característica es cero o primo.

**Ejemplo 1.10.1**. Un ejemplo claro de la característica de un campo es cuando se considera el campo $\mathbb{Z}_2$ note que en este campo claramente $\bar{1} + \bar{1} = \bar{0}$ por tanto la característica existe y es igual a 2. De igual forma con $\mathbb{Z}_3$ ya que $\bar{1} + \bar{1} + \bar{1} = \bar{3} = \bar{0}$

**Propiedad 1.11**. El número de elmentos de un campo finito $\mathbb{Z}_{\text{ı}}[x]/(p(x))$ es $p^n$ donde $n$ es el grado de $p(x)$.

**Ejemplo 1.11.1**. Un ejemplo facíl es cuando pensamos en el campo $\mathbb{Z}_2/(\bar{1} + x + x^2)$. Aquí $p = 2$ y $n = 2$ por tanto el número de elementos de dicho campo es $p^n = 2^2 = 4$ lo cual ya hemos visto que sí se cumple.

**Campo de Galois 1.11.2**. Un campo finito con $p^m$ elementos se llama un **campo de Galois** de order $p^m$ y se denota por $GF(p^m)$. Se puede demostrar que dado un número primo $p$ y un entero positivo $m$, un campo de Galois $GF(p^m)$ existe y además todos los campos de orden $p^m$ son isomorficos. Un ejemplo en particular, para $m = 1$, los enteros modulo $p$, $\mathbb{Z}_p$, es un campo de Galois de orden $p$. También se cumple que $GF(p^m)$ es una extención de campo para $\mathbb{Z}_p$ de grado $m$. Todo campo finito $GF(p_m)$ puede contruírse encontrando un polinomio $q(x)$ de grado $m$, irreducible de $\mathbb{Z}_p[x]$, definimos pues:

$$GF(p^m) = Z_p[x]/(q(x)).$$

**Ejemplo 1.11.3**. Como ejemplo se puede considerar al campo $K = \mathbb{Z}_{\not\in}/(\bar{1} + x + x^2)$, ya que como dice la definición, se cumple $K$ tiene $2^2$ elementos.

**Definición 1.12**. Podemos ahora definir el anillo de polinomios en las $n$ variables $x_1, \cdots, x_n$ sobre $R$, $R[x_1, \cdots, x_n]$. Notemos que sus elementos son de la siguiente forma

$$\Sigma a_{i_1 i_2 \cdots i_n} x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}.$$

**Ejemplo de Operaciones 1.12.1**. Aquí la igualdad y la suma son definidas por los coeficientes, sin embargo la multiplicaión esta dada por la ley distributiva y la regla de los exponentes

$$(x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n})(x_1^{j_1} x_2^{j_2} \cdots x_n^{j_n}) = x_1^{i_1+j_1} x_2^{i_2+j_2} \cdots x_n^{i_n+j_n}.$$

**Ejemplo 1.12.2**. Veamos un ejemplo de como sería un polinomio de variable multiple para $n = 2$. Así como en la parte de arriba se obtiene que $R_1 = R[x]$ donde $R$ es un anillo, luego $R_2 = R_1[x_2]$ y por tanto podemos expresar sus elementos de la forma:

$$\phi \in R_2 \text{ implica que } \phi = \Sigma a_{ij} x^i x^j = \sum_{i=0}^{n} \sum_{j=0}^{m} a_{ij} x^i y^j$$

$$= \sum_{j=0}^{m} (\sum_{i=0}^{n} a_{ij} x^i) y^j = \sum_{j=0}^{m} (a_{0j} + a_{1j} x + \cdots + a_{nj} x_n) y^j$$

$$= \sum_{j=0}^{m} (p_j(x)) y^j = p_0(x) + p_1(x) y + \cdots + p_m(x) y^m.$$

Para evitar confución note que $p_j(x) = a_{0j} + a_{1j} x + \cdots + a_{nj} x_n$, $\forall j = 0, \cdots, m$. Ahora veremos algunas propiedades que se cumlpen para polinomios de variable multiple.

## 2. Criptografía de Variable Multiple

**Definicion 2.1**. La Criptografía de Variable Multiple es el estudio de los MPKCs donde la función trampa toma la forma de un polinomio cuadratico multivariable sobre un campo finito. En general la llave publica esta dada por un conjunto de polinomios cuadraticos:

$$P = (p_1(w_1, \cdots, w_n), \cdots, p_n(w_1, \cdots, w_n)),$$

en donde cada $p_i$ es un polinomio (usu. cuadrático) no lineal en $\mathbf{w} = (w_1, \cdots, w_n)$:

$$z_k = p_k(\mathbf{w}) = \sum_i P_{ik} w_i + \sum_i Q_{ik} {w_i}^2 + \sum_{j<i} R_{ijk} w_i w_j$$

**¿Qué es un MPKC?**. Multivariate public key cryptosystem (MPKCs siglas) tienen un conjunto (aveces) de polinomios cuadraticos sobre un campo finito como su clave pública. Esto se apoya en un problema de dificultad NP de resolver ecuaciones no lineales sobre un campo finito. Esta tipo de seguridad es parte de los MPKCs que pueden llegar a resistir ataques fuertes de computadores cuanticas del futuro.

**Problema 2.1.1**. Resuelva el sistema $p_1(\mathbf{x}) = p_1(\mathbf{x}) = \cdots = p_m(\mathbf{x}) = 0$, donde cada $p_i$ es cuadrático en $\mathbf{x} = (x_1, \cdots, x_n)$. Todos los coeficientes y variables estan en $\mathbb{K} = \mathbb{F}_q$, con $q$ elementos.

**Encriptación 2.2**. Considere una llave publica dada por:

$$S(x_1, \cdots, x_n) = (p_1(x_1, \cdots, x_n), \cdots, p_m(x_1, \cdots, x_n)).$$

Aquí los $p_i(x_1, \cdots, x_n)$ son polinomios multivariables sobre un campo finito. Dado cualquier texto plano $M = (x'_1, \cdots, x'_n)$ este se cifra mediantela regla:

$$S(M) = S(x'_1, \cdots, x'_n) = (y'_1, \cdots, y'_m)$$

Para decifrar $(y'_1, \cdots, y'_m)$, se necesita la llave secreta para poder invertir el mapeo $S^{-1}$ y así encontrar el text plano $M$.

**Ejemplo 2.1.2**. Ahora veamos un caso particular. Usemos el conjunto cociente

$$K = GF(2)/(x^2 + x + 1).$$

Ya vimos que $GF(q^m) = \mathbb{Z}_q[x]/(p(x))$ por tanto en este caso $GF(2) = \mathbb{Z}_2[x]/(p(x))$ y ya hemos trabajado con $K$ en ejemplos anteriores. Por tanto sabemos que $K$ tiene $2^2$ elementos y dado que $p(x) \in \mathbb{Z}_2$ se cumple que $p(x)$ es irreducible en $\mathbb{Z}_2$. Por teoremas anteriores se obtiene que $K$ es un campo finito y además es de la forma

$$K = \{(p(x)), (p(x)) + 1, (p(x)) + x, (p(x)) + x + 1\}.$$

Ya tenemos todas las posibles operaciones para suma y multiplicación del campo $K$, entonces dado nuestro texto plano $M = (k_0, k_1, k_2)$ donde $k_0, k_1, k_2 \in K$ podemos evaluar en un campo de polinomios en tres variables. En este caso en particular se considera $n = 3$ y definimos $K_1 = K[x_1]$, $K_2 = K_1[x_2]$ y finalmente $K_3 = K_2[x_3]$. Veamos como serían los elementos de $K_3$:

$$\text{Un elemento en } K_3 \text{ tiene la forma } \sum a_{ijk}x^iy^jz^k$$

$$= \sum_{i=0}^{n}\sum_{j=0}^{m}\sum_{k=0}^{l} a_{ijk}x^iy^jz^k = \sum_{k=0}^{l}[\sum_{j=0}^{m}(\sum_{i=0}^{n} a_{ijk}x^i)y^j]z^k$$

$$= \sum_{k=0}^{l}[\sum_{j=0}^{m}(a_{0jk} + \cdots + a_{njk}x^n)y^j]z^k$$

$$= \sum_{k=0}^{l}[(a_{00k} + \cdots + a_{n0k}x^n) + (a_{01k} + \cdots + a_{n1k}x^n)y + \cdots + (a_{0mk} + \cdots + a_{nmk}x^n)y^m]z^k$$

$$= \sum_{k=0}^{l}[q(x)_0 + q_1(x)y + \cdots + q_m(x)y^m]z^k$$

$$= (q(x)_0 + q_1(x)y + \cdots + q_m(x)y^m) + (q(x)_0 + q_1(x)y + \cdots + q_m(x)y^m)z + \cdots + (q(x)_0 + q_1(x)y + \cdots + q_m(x)y^m)z^l$$

$$= r_0(x,y) + r_1(x,y)z + \cdots + r_l(x,y)z^l = \phi(x,y,z)$$

Ya sabemos como operar en $K$ y además conocemos como son los elementos de $K_3$, por tanto podemos elegir los polinomios $S_0(x,y,z), S_1(x,y,z), S_2(x,y,z) \in K_3$ dados por:

$$S_0(x,y,z) = 1 + z + 2xz + 3y^2 + 3yz + z^2,$$

$$S_1(x,y,z) = 1 + 3x + 2y + z + x^2 + xy + 3xz + y^2,$$

$$S_2(x,y,z) = 3z + x^2 + 3y^2 + yz + 3z^2,$$

se utiliza la notación $(p(x)) = 0$, $(p(x)) + 1 = 1$, $(p(x)) + x = 2$ y $(p(x)) + x + 1 = 3$. Además considere para este ejemplo el texto plano $M = ((p(x)) + 1, (p(x)) + x, (p(x)) + x + 1) = (1, 2, 3)$. Entonces se tiene que nuestra llave pública esta dada por:

$$S(x,y,z) = (S_0(x,y,z), S_1(x,y,z), S_2(x,y,z))$$

Por tanto evaluamos nuestro texto plano $M$ en $S$ como sigue:

$$\begin{aligned} S(M) = S(1,2,3) = (&1 + 3 + 2(1)(3) + 3(2)^2 + 3(2)(3) + (3)^2,\\ &1 + 3(1) + 2(2) + 3 + (1)^2 + (1)(2) + 3(1)(3) + (2)^2,\\ &3(3) + (1)^2 + 3(2)^2 + (2)(3) + 3(3)^2)\\ &= (0,0,1). \end{aligned}$$

Así pues se cumple que dado el texto plano $M = (1,2,3)$ nuestra llave pública arroja el texto cifrado $S(M) = (0,0,1)$.

**Firma 2.3**. Para poder firma el valor del documento hash $(y'_1, \ldots y'_m)$, uno necesita saber **la llave secreta** y así poder invertir la llave pública $S^{-1}$ para poder encontrar la firma $(x'_1, \ldots x'_n)$.

$$S = (x'_1, \ldots x'_n) = S^{-1}(y'_1, \ldots y'_m).$$

Entonces dado la pareja:

$$((x'_1, \ldots x'_n), (y'_1, \ldots y'_m)),$$

cualquiera puede verificar la validez de la firma revisando si se cumple la igualdad

$$S(x'_1, \ldots x'_n) = (y'_1, \ldots y'_m).$$

**Fundamento Teórico 2.4**. Si se pide saber el fundamento teórico del porque optar por este sistema note lo siguiente:

1. Un ataque directo consiste en solucionar el conjunto de ecuaciones:

$$S(M) = S(x'_1, \dots x'_n) = (y'_1, \dots y'_m)$$

2. Al momento de resolver una cantidad $n$ de ecuaciones (no lineales) de $n$ variables es NP-completo, aunque esto no necesariamente asegura la seguridad de los sistemas.

## 3. Esquema de Firma Rainbow

**Introducción 3.1**. Ya hemos visto como son los polinomios multivariables sobre un campo finito y como se operan sobre el, en esta sección vamos a utilizar conceptos de las secciones anteriores para así poder introducir la generalización para la construcción del sistema de autenticacón Oil-Vinegar (Aceite y Vinagre en español). Un punto clave es la construcción de un sistema Oil-Vinegar multi-capa, el cual se le llama **Rainbow**.

**Fundamento Teórico 3.2**. Unas de las construcciones que se han perseguido en el campo de los sistemas de cifrado multivariables seguros son Oil and Vinegar y Unbalanced Oil Vinegar. Para la construcción de estos esquemas se utiliza la idea de que algunas ecuaciones cuadráticas se pueden resolver de una forma relativamente facíl si se nos permite adivinar algunas variables. Por ejemplo, consideré un campo finito $K$. Aquí la clave es la construcción de un mapa $F$ de $K^{o+v}$ a $K^o$: es decir

$$F(x_1, \dots, x_o, x'_1, \dots, x'_v) = (F_1(x_1, \dots, x_o, x'_1, \dots, x'_v), \dots, F_o((x_1, \dots, x_o, x'_1, \dots, x'_v)$$

cabe destacar que cada $F_l$ es de la forma:

$$F_l((x_1, \dots, x_o, x'_1, \dots, x'_v) = \sum a_{lij} x_i x'_j + \sum b_{lij} x'_i x'_j + \sum c_{li} x_i + \sum d_{lj} x'_j + e_l,$$

donde $x_i$, $i = 1, \dots, o$, se llaman las variables Oil (Aceite) y $x_j$, $j = 1, \dots, v$, son llamados las variables Vinegar (Vinagre) en el campo finito $K$. A los polinomios de este tipo se les llama **polinomios de Aceite y Vinagre** . La razón por la cual se les llama polinomios de Aceite y Vinagre es por que las variables de Aceite y Vinagre en el campo finito $K$ no esta enteramente mixtas, esto nos permite encontrar una solución facíl para cualquier ecuación de la forma:

$$F(x_1, \dots, x_o, x'_1, \dots, x'_v) = (y_1, \dots, y_o)$$

dado $(y_1, \dots, y_o)$. Esta clase de ecuación ya se estudio en la sección anterior. Para poder encontrar una solución es necesario ingresar variables Vinagre en el campo finito $K$ aleatorias en la ecuación anterior. La probabilidad de elegir las variables Vinagre correctas es cercano a 1, en dado caso de que nos equivoquemos al elegir las viarbles correctas solo basta intentar de nuevo. Esta familia de cifrados se diseñarón especificamente para esquemas de firma, en donde solo necesitamos encontrar una solución y no una única solución. Una vez que se define este mapa $F$ se esconde haciendo una composición por la izquierda y derecha utilizando tranformaciones lineales afines $L_1$ y $L_2$. Se debe de cumplir que $L_1$ esta sobre $K^o$ y que $L_2$ este sobre $K^{o+v}$, esto nos genera un mapa cuadrático de $K^{o+v}$ a $K^o$:

$$\bar{F} = L_1 \circ F \circ L_2,$$

**Observaciones 3.2.1.** Primero se considero el esquema Aceite y Vinagre en donde $v = o$, sin embargo pero fue derrotado por Kipnis y Shamir usando matrices relacionadas a formas bilineales definidas por polinomios cuadraticos. Ahora cuando se trabaja con Aceite y Vinagre desiquilibrado i.e. $v > o$, se demostro que en un ataque especifico tiene una complejidad de alrededor de $q^{v-o-1}o^4$, cuando $v$ es casi igual a $o$. Esto quiere decir que caundo $o$ no es muy grande ($< 100$) y dado un campo de tamaño q, entonces $v - o$ debería de ser suficientemente grande, pero no tan grande, para afirmar la seguridad del sistema. Cabe mencionar que en este esquema el documento a firmar es un vector en $k^o$ y la firma es el vector $K^{o+v}$, esto significa que la firma es almenos el doble de tamaño que el del documento y con un sistema de tamaño $v + o$ este se vuelve más eficiente.

**Rainbow 3.3.** Ahora veamos la construcción del Rainbow de forma general. Sea $S$ el conjunto $\{1, 2, 3, \ldots, n\}$ y consideramos enteros $v_1, \ldots v_u \in S$ tales que $0 < v_1 < v_2 < \ldots < v_u = n$, luego definimos los conjuntos $S_l = \{1, 2, 3, \ldots, v_l\}$ para $l = 1, \ldots, u$, entonces se tiene que

$$S_1 \subset S_2 \subset \cdots \subset S_u = S$$

Note que el número de elementos de $S_i$ es $v_i$. Definimos también alos enteros

$$o_i = v_{i+1} - v_i, \text{ para } i = 1, \ldots, u - 1.$$

De igual manera se definen los conjuntos $O_i$ tales que

$$O_i = S_{i+1} - S_i, \, \forall i = 1, \ldots, u - 1.$$

Para $l = 1, 2, 3, \ldots, u$ sea $P_l$ el espacio líneal generado por por los polinomios de la forma:

$$\sum_{i \in O_l, j \in S_l} \alpha_{ij} x_i x_j + \sum_{i,j \in S_l} \beta_{ij} x_i x_j + \sum_{i \in S_{l+1}} \gamma_i x_i + \eta.$$

A los polinomios en $P_l$ se les llama polinomios de $l$-esima capa de Aceite y Vinagre. Ademas es facíl ver que también $P_i \subset P_j$ para cualesquiera, $i < j$. Entonces se puede decir que cada polinomio en $P_l$ tiene a $x_i$ como una varible aceite si $i \in O_l$ y a $x_i$ como una variable de Vinagre si $i \in S_l$. La separación de las variables aceite y vinagre se vuelve más notorio cuando nos damos cuenta de que $S_{i+1} = S_i \cup O_i$.

**Ejemplo 3.3.1.** Veamos un ejemplo de como construí nuestro propio esquema de polinomios aceite y vinagre. Elegimos $S = \{1, 2, 3, 4, 5, 6, 7\}$ y sean $v_1 = 2, v_2 = 4, v_3 = 6$ y finalmente $v_4 = 7$. Entonces se cumple que $0 < v_1 < v_2 < v_3 < v4 = 7$. Portanto ya podemos definir los conjuntos $S_1 = \{1, 2\}$, $S_2 = \{1, 2, 3, 4\}$, $S_3 = \{1, \ldots, 6\}$ y $S_4 = S$, luego podemos ver que $S1 \subset S_2 \subset S_3 \subset S_4 = S$. Estos como ya hemos dicho estan relacionados a las variables Vinagre. En este caso $u = 4$ y además definimos al indice $l \in \{1, \ldots, 4\}$ Entonces ya que $u = 4$ podemos ahora definir los conjuntos $O_i$'s (con $i = 1, \ldots, u - 1$) relacionados a las variables Aceite. Siguiendo el procedimiento de arriba tenemos que $o_1 = 2, o_2 = 2$ y $o_3 = 1$, luego se sigue que $O_1 = \{3, 4\}, O_2 = \{5, 6\}$ y $O_3 = \{7\}$. Se verifica que v¿o como se había dicho en la sección pasada. Ahora ya estamos listo para ver como es un polinomio de $l - esima$ capade Aceite y Vinagre. Para ejemplificar sea $l = 1$, luego se cumple que:

$$\sum_{i \in O_1, j \in S_1} \alpha_{ij} x_i x_j + \sum_{i,j \in S_1} \beta_{ij} x_i x_j + \sum_{i \in S_2} \gamma_i x_i + \eta =$$
$$\sum_{i=3}^{4} \sum_{j=1}^{2} \alpha_{ij} x_i x_j + \sum_{i=1}^{2} \sum_{j=1}^{2} \beta_{ij} x_i x_j + \sum_{i=1}^{4} \gamma_i x_i + \eta,$$

aquí desarrollamos cada termino del polinomio por separado:

$$\sum_{i=3}^{4}\sum_{j=1}^{2}\alpha_{ij}x_ix_j = \sum_{i=3}^{4}(\alpha_{i1}x_ix_1 + \alpha_{i2}x_ix_2) = \alpha_{31}x_3x_1 + \alpha_{32}x_3x_2 + \alpha_{41}x_4x_1 + \alpha_{42}x_4x_2$$

$$\sum_{i=1}^{2}\sum_{j=1}^{2}\beta_{ij}x_ix_j = \sum_{i=1}^{2}(\beta_{i1}x_ix_1 + \beta_{i2}x_ix_2) = \beta_{11}x_1^2 + \beta_{12}x_1x_2 + \beta_{21}x_2x_1 + \beta_{22}x_2^2$$

$$\sum_{i=1}^{4}\gamma_ix_i = \gamma_1x_1 + \gamma_2x_2 + \gamma_3x_3 + \gamma_4x_4.$$

**Esquema de la Firma Rainbow 3.4.** Ahora podemos definir un mapa $F$ del esquema de firma de Rainbow, el cual es un mapa de $K^n$ a $K^{n-v_1}$ tales que

$$\begin{aligned} F(x_1,\ldots,x_n) &= (\bar{F}_1(x_1,\ldots,x_n),\ldots,\bar{F}_{u-1}(x_1,\ldots,x_n)) \\ &= (F_1(x_1,\ldots,x_n),\ldots,F_{n-v_1}(x_1,\ldots,x_n)), \end{aligned}$$

cada uno de los $\bar{F}_i$ consiste de $o_i$ polinomios cuadraticos elegidos al azar del espacio lineal de polinomios $P_i$. Siempre se pueden elegir polinomios al azar al elegir su coeficientes al azar. Entonces se puede ver a los $\bar{F}_i$ de la siguiente forma:

$$\begin{gathered} \bar{F}_1 = (F_{v_1+1},\ldots F_{v_2}), \text{ ya que } O_1 = \{v_1,\ldots,v_2\} \\ \bar{F}_2 = (F_{v_2+1},\ldots F_{v_3}),\ O_2 = \{v_2,\ldots,v_3\} \\ \vdots \\ \bar{F}_{u-1} = (F_{v_{u-1}+1},\ldots F_{v_n}),\ O_{u-1} = \{v_{u-1},\ldots,n\}. \end{gathered}$$

Podemos observar que la $i_esima$ capa de $o_i$ polinomios son de la forma $F_{v_i+1},\ldots,F_{v_{i+1}}$ tales que $x_j$, con $j \in O_i$ son las variables Aceite y $x_i$ con $j \in S_i$ son las vairables Vinagre. De aquí podemos definir nuestro .ªrcoiris"de variables de la siguiente manera:

$$\begin{gathered} x_1,\ldots,x_{v_1};\ x_{v_1+1},\ldots,x_{v_2} \\ x_1,\ldots,x_{v_1},x_{v_1+1},\ldots,x_{v_2};\ x_{v_2+1},\ldots x_{v_3} \\ x_1,\ldots,x_{v_1},x_{v_1+1},\ldots,x_{v_2},x_{v_2+1},\ldots x_{v_3};\ x_{v_3+1},\ldots,x_{v_4} \\ \vdots \\ x_1,\ldots,\ldots,\ldots,\ldots,\ldots,\ldots,\ldots,\ldots,\ldots,\ldots,\ldots,\ldots,x_{v_{u-1}};\ x_{v_{u-1}},\ldots,x_n. \end{gathered}$$

En cada fila los del lado izquierdo se llaman las variables Vinagre y los del lado derecho se llaman variables Aceite. Finalmente llamamos al mapa $F$ un polinomio Arcoiris de $u-1$ capas. Finalmente se eligen dos transformaciones lineales afines $L_1$ y $L_2$ donde $L_1$ esta sobre $K^{n-v_1}$ y $L_2$ esta sobre $K^n$. Entonces se define el mapa:

$$G(x_1,\ldots,x_n) = L_1 \circ F \circ L_2(x_1,\ldots,x_n),$$

el cual consiste de $n - v_1$ polinomios cuadraticos en $n$ variables.

# 4. El Cifrado de Matsumoto-Imai

**Introducción 4.1**. En esta sección veremos otro criptosistema que se basa en polinomios multivariables sobre un campo finito, en particular se trabaja con polinomios cuadraticos. Veremos un sistema que fue desarrollado por Matsumoto y Imai y del cual hay dos versiones. La primera fue derrotada por un ataque algebaríco utilizando la linearizacion de ecuaciones de Patarin. La segunda versión se llama la perturbación de Matsumoto-Imai el cual fue modificado y trabajado por Patarin y sus colaboradores. Nuevamente al igual que el sistema Rainbow mencionado en la sección anterior, el sistema de Matsumoto-Imai depende del teorema que nos garantiza que para resolver un conjunto de polinomios sobre un campo finito es un problema de dificultad NP. Sin embargo esto no garantiza su seguridad.

En el sistema original de Matsumoto-Imai ellos proponen el uso de un mapa $F$ sobre un campo grande $K$ el cual debe ser una extensión de grado $n$ de un campo finito $k$. Vamos a identificar a $K$ como $k^n$ atravez de un mapeo $F$, luego se puede definir un mapeo de $k^n$ a $k^n$ denotado por $\tilde{F}$ el cual sería un mapeo multivariable. El paso siguiente sera esconder este mapeo utilizando una composición de funciones de la siguiente forma:

$$\bar{F} = L_1 \circ \tilde{F} \circ L_2$$

donde $L_1$ y $L_2$ son transformaciones lineales affines sobre $k^n$. Aquí Matsumoto y Imai proponen un mapeo $F$ en particular el cual pertenece a la primera versión que fue derrotada por los ataques algebraícos de Patarin como ya se mencionó antes. El mapeo $F$ que sugirierón Matsumoto y Imai fue:

$$F : X \mapsto X^{1+q^i},$$

en donde $q$ es el número de elementos en en el campo finito $k$, $X$ pertenece al campo $\bar{K}$ y $k$ es de caracteristica 2. Despues de que fue derrotado el primer sistema de Matsumoto-Imai se hicieron modificaciones para así poder extender el primer sistema y se constan de tres modificaciones: el metodo Menos-Mas, el metodo de ecuación de campo escondido y el metodo de ecuación de campo escondido con el metodo Aceite-Vinagre.

**Extensión del Sistema Matsumoto-Imai 4.2.** Veamos como es que el sistema de Matsumoto se extendio despues de su derrota. Como ya se mencionó el sistema fue extendido de tres formas:

1. **Metodo Menos-Más**. Este metodo consta de quitar polinomios cuadraticos que son componentes del mapeo $\bar{F}$ o de agregarle polinonomios cuadraticos, ambos al azar. Aquí cabe mencionar que se sugiere usar el metodo de solo quitar polinomios por razones de seguridad, en especial para los esquemas de firmas.

2. **Metodo de Ecuación de Campo Escondido**. El HFE (siglas en íngles) metodo es muy parecido al sistema original de Matsumoto-Imai y solo difiere en que el mapeo $F$ es reemplazado por el mapeo:

   $$F : X \mapsto \sum_{i,j}^{A} a_{ij} X^{q^i+q^j} + \sum_{i}^{B} b_i X^{q^i} + c,$$

   aquí los coeficientes se eligen de forma aleatoria y el grado de $F$ debe de ser pequeño ya que sino el proceso de decifrado será muy lento. Patarin menciona que de los tres metodos este es

el más fuerte, pero un ataque algebraíco llevado acabo por Kipnis y Shamir demostro que $A$ no puede ser muy pequeño, ni tampoco puede ser muy grande ya que el sistema se alenta y se debe a que al resolver la ecuación polinomial el proceso de decifrado se alenta.

3. **Metodo de Ecuación de Campo Escondido con el Metodo Aceite-Vingre**. Aquí se trabaja encima del HFE reemplazando a $F$ con otro mapeo más complejo:

   $$F : (X, \bar{X}) \mapsto \sum_{i,j}^{A} a_{ij} X^{q^i+q^j} + \sum_{i,j}^{B,B'} b_{ij} X^{q^i} \bar{X}^{q^j} + \sum_{i,j}^{A'} \alpha_{ij} \bar{X}^{q^i+q^j} + \sum_{i,j}^{B'} \beta_i' \bar{X}^{q^i} + \sum_{i,j}^{B} b_i X^{q^i} + c,$$

   es recomendable que la nuevas variable vinagre dadas por la variable $\bar{X}$ sea de dimensión pequeña. Cuando se trate de esquema de firma la busqueda de la nuevas variable agregadas se vuelve una cuestión del selección al azar con buena probabilidad de exito. Pero de forma general la busqueda de las nuevas variables debe de ser exhuasitiva. Note que en este metodo se puede interpretar como una perturbación de un sistema pequeño a una escala pequeña, de ahí el nombre del sistema.

Note que en el tercer metodo al agregarle variables nuevas esto se puede interpretar como una perturbación externa. Ay que aclarar que en si lo que se busca es una perturbación interna, entonces la perturbación debe de llevarse acabo dentro de un subconjunto pequeño de $k^n$. Es decir, dado un sistema cuadrático multivariable $\bar{F}$ sobre $k^n$, se busqua al azar un transformación lineal afín sobreyectiva $Z$ de $k^n$ a $k^n$ con una dimensión pequeña $r$. Luego al jugar con el número pequeño de elementos correspondientes a $Z$ es como se logra la perturbación interna. Este es un cuarto metodo propuesto por Jintai Ding.

**Metodo de Perturbación Oculta en una Ecuación 4.3.** El proceso de perturbación se lleva acabo en dos partes.

1. El primer paso es elegir al azar $r$ funciones linealemente independientes de la siguiente forma:

   $$z_i = \sum_i^n \alpha_{ij} x_i + \beta_i,$$

   aquí las variables $x_i$ son las variables de $\bar{F}$, los cuales se pueden ver como las variables de $\tilde{F}$ y se pueden manejar como las componentes suprayectivas de mapeo lineal afín $Z$ que va de $k^n$ a $k^r$.

2. El segundo paso y ultimo paso consta de sumarle a las componentes de $\tilde{F}$ un polinomio cuadrático formado por los $z_i$ de forma aleatoria y así mismo definir una nuevo mapa $G$ para reemplazar a $\tilde{F}$, es decir:

   $$G(x_1, \ldots, x_n) = (\tilde{F}_1(x_1, \ldots, x_n) + f_1(z_1, \ldots, z_r), \ldots, \tilde{F}_n(x_1, \ldots, x_n) + f_n(z_1, \ldots, z_r))$$

   .

Aquí cabe mencionar que ya no podemos aplicarle el tercer metodo ya que no hay terminos lineales que mezclan los terminos Aceite-Vinagre. Aún así el sistema no es completamente seguro pero podría soportar ataque algebraícos existentes tales como los de Kipnis y Shamir.

**Construccion y Ejemplo de Matsumoto-Imai 4.4.** Primer vamos a empezar por construír el sistema original de Matsumoto-Imai. Para esto se necesita de un campo finito $k$ de characteristica 2 (aunque no necesariamente) con $q$ elementos. Sea $\bar{K}$ un extensión de campo de $k$ de grado $n$ tal que

$$\bar{K} \equiv k[x]/g(x).$$

Antes de continuar hagamos una aclaración, para poder visualizar lo que esta ocurriendo trabajaremos con un campo finito ya muy conocido para nosotros, aunque todo lo que desarrollemos funciona análogamente para otros campos finitos. Sea pues $\bar{K} = \mathbb{Z}_2[x]/(\bar{1} + x + x^2)$, note que entonces $k = \mathbb{Z}_2$ es de característica 2, tiene $q = 2$ elementos y sea

$$g(x) = \bar{1} + x + x^2,$$

y ya hemos visto que $g(x)$ es irreducible en $\mathbb{Z}_2$ y por tanto $I = (g(x))$ es un ideal. Ahora, sea $\phi$ el mapa k-lineal estandar que identifica a $\bar{K}$ con $k^n$ tal que

$$\phi(I + a_0 + a_1x + \cdots + a_{n-1}x^{n-1}) = (a_0, \ldots, a_{n-1}).$$

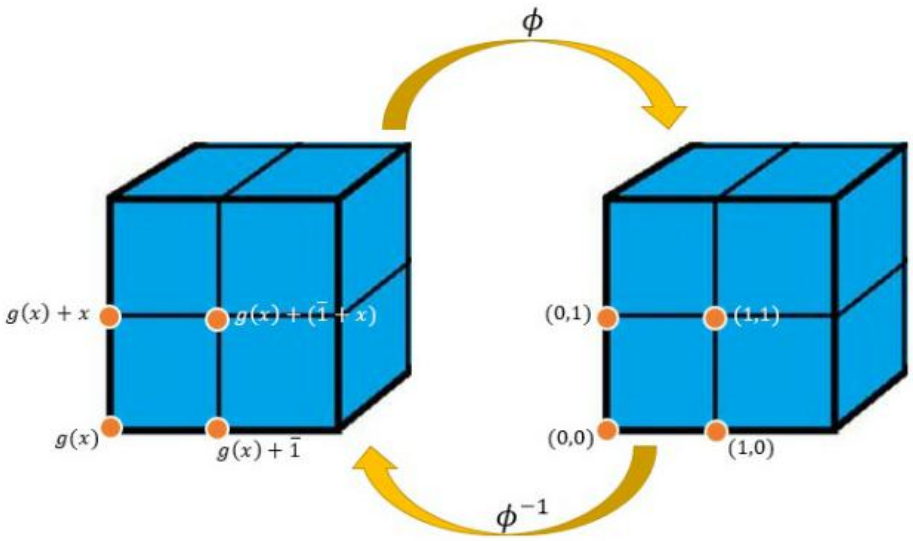


Figura 1: $\phi$ para $\bar{K} = \mathbb{Z}_2[x]/(\bar{1} + x + x^2)$

Así como se ve en la figura 1 podemos ver que dado dos $a_0$ y $a_1$ en $\mathbb{Z}_2$ se le asigna un único elemento $X = I + a_0 + a_1x \in \bar{K}$ y vice versa. Ahora sea

$$F(X) = X^{1+q^i}, \text{ tal que } X \in \bar{K}$$

y en donde $t(1 + q^i) \equiv 1 \ (mod\ q^n - 1)$. Sin embargo para nuestro ejemplo tenemos que

$$F(X) = X^{1+2^i} \text{ tal que } t(1 + 2^i) \equiv 1 \ mod(2^n - 1).$$

$$\text{en donde } t(1 + 2^i) \equiv 1 \ mod\ 3,$$

Entonces ya solo es cuestión de elegir un $i$ adecuado tal que $(1+2^i, 3) = 1$. Por ejemplo se podría elegir $i = 4$ y así tendríamos que $F(X) = X^{1+2^4} = X^{17}$.

Continuando con el desarrollo, ya que tenemos la forma k-lineal estandar podemos definir un mapeo de $k^n$ a $k^n$. En nuestro ejemplo de $\bar{K} = \mathbb{Z}_2[x]/(\bar{1} + x + x^2)$ dado $\gamma = (a_0, a_1) \in k^2$ podemos aplicar $\phi^{-1}$ y así obtener $\phi^{-1}(a_0, a_1) = I + (a_0 + a_1 x)$. Aquí mismo aplicamos

$$F(\phi^{-1}(a_0, a_1)) =$$
$$F(I + (a_0 + a_1 x)) =$$
$$(I + (a_0 + a_1 x))^{1+q^i} =$$
$$I + (a_0' + a_1'),$$

el cual sigue perteneciendo a $\bar{K}$, luego se aplica $\phi$

$$\phi(F(\phi^{-1}(a_0, a_1))) =$$
$$\phi(F(I + (a_0 + a_1 x))) =$$
$$\phi((I + (a_0 + a_1 x))^{1+q^i}) =$$
$$\phi(I + (a_0' + a_1')) =$$
$$(a_0', a_1') \in k^n.$$

Entonces lo que ha sucedido se puede expilcar por medio de la figura 2. Si cada $(a_0, a_1) \in k^n$ representa un cubo $A_{a_0 a_1}$ cuyo lugar es $(a_0, a_1)$, entonces cuando se aplica $\phi^{-1}$ le estamos asignando un elemento de $\psi = \mathbb{Z}_2/I$ a dicho cubo. Luego con $F$ multiplicamos a $\psi$ $1+2^i$ veces por si mismo y entonces nuestro cubo $A_{a_0 a_1}$ ahora esta en correspondencia con $F(\psi)$ y por tanto ahora le pertenece el lugar $\phi(F(\psi)) = (a_0', a_1')$ y se mueve a esa nueva coordenada.

Teniendo ya una imagen más clara de lo que esta sucediendo podemos ahora sí definir el mapeo $\tilde{F}$ como

$$\tilde{F} = \phi \circ F \circ \phi^{-1} =$$
$$(\tilde{F}_1(x_1, \ldots, x_n), \tilde{F}_2(x_1, \ldots, x_n), \ldots, \tilde{F}_n(x_1, \ldots, x_n)).$$

Para nuestro ejemplo de $F = X^{17}$ se cumple que

$$\tilde{F} = (\tilde{F}_0, \tilde{F}_1), \text{ en donde}$$
$$\tilde{F}_0(a_0, a_1) = a_0' \text{ y } \tilde{F}_1(a_0, a_1) = a_1'$$

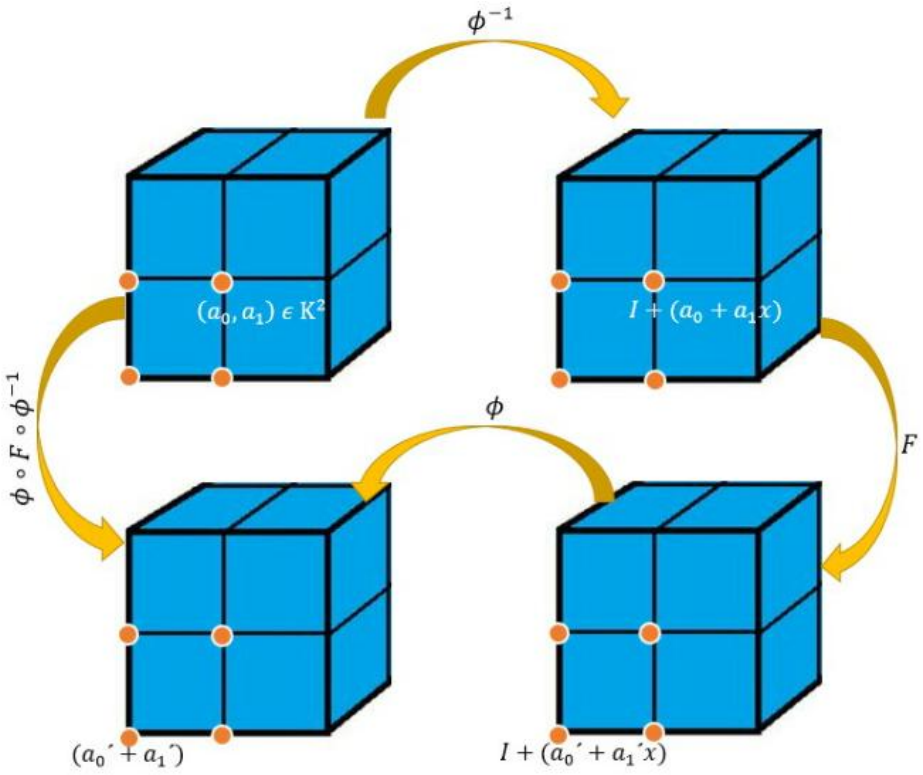


Figura 2: Dinámica de $\tilde{F} = \phi \circ F \circ \phi^{-1}$

Se cumple que los $\tilde{F}_i(x_1, \ldots, x_n)$ son polinomios cuadraticos de $n$ variables. Para terminar se eligen al azar $L_1$ y $L_2$ dos mapeos lineales afines sobre $k^n$

$$\bar{F}(x_1, \ldots, x_n) = L_1 \circ \tilde{F} \circ L_2(x_1, \ldots, x_n) =$$
$$(\bar{F}_1(x_1, \ldots, x_n), \bar{F}_2(x_1, \ldots, x_n), \ldots, \bar{F}_n(x_1, \ldots, x_n)),$$

este cifrado fue sugerido por Matsumoto-Imai, sin embargo fue derrotado por ataques algebraícos por parte de Patarin.

**Visualización de $\bar{K} = \mathbb{Z}_2[x]/(\bar{1} + x + x^2)$ 4.5.**Para poder aterrizar mejor la idea de los campos finitos y ver de donde vienen nuestras llaves veamos estudiemos la relación entre el toro de dimensión 2 y el campo $\bar{K}$. El conjunto $\bar{K}$ tiene una estructura similar a la figura 3

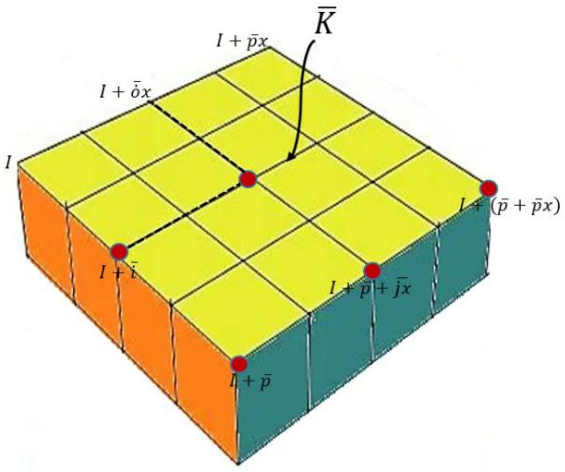


Figura 3: $\bar{K} = \mathbb{Z}_2[x]/(\bar{1} + x + x^2)$ como una red.

entonces con la ayuda del mapa k-lineal estandar $\phi$ ya se se puede ver a $\bar{K}$ como $k^2$ y se muestra en la figura 4.

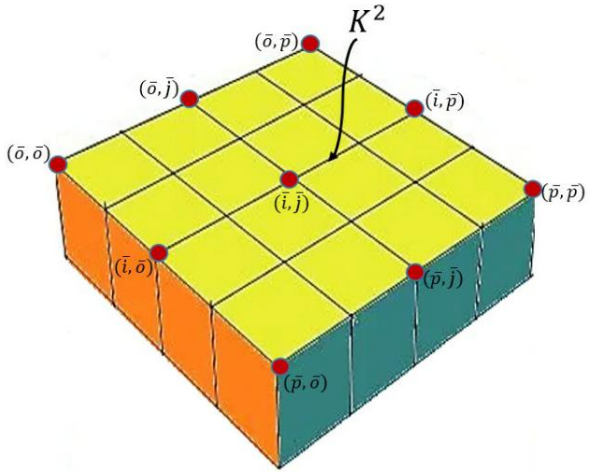


Figura 4: $\bar{K}$ visto como $k^n$.

Ahora definimos la biyección $\psi : k^p \mapsto I^p$ dada por

$$\psi(\bar{i}, \bar{j}) = (\tfrac{2\pi i}{p}, \tfrac{2\pi j}{p}),$$

donde $p$ es un primo y $I = \{0, \frac{2\pi}{p}, \ldots, 2\pi\}$. Aunque para nuestro caso solo estamos considerando $p = 2$. Luego el mapeo $\psi$ se puede observar como viene en la figura 5.

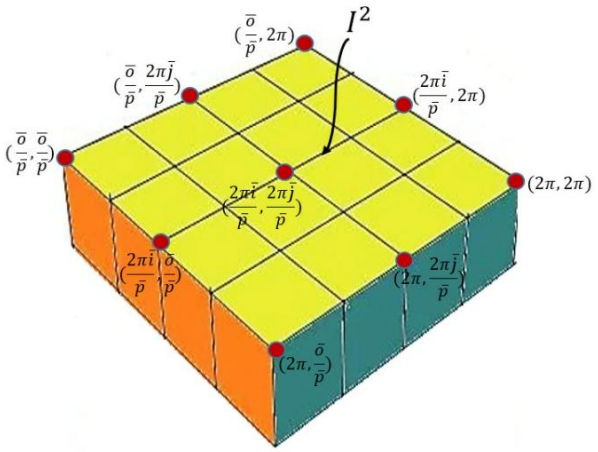


Figura 5: $\bar{K}$ visto como $k^n$.

Finalmente llegamos al ultimo paso consideré el mapeo $Torus : I^2 \mapsto \mathbb{R}^3$ dado por la regla

$$Torus(i_I, j_I) = ((R - rcosj_I)cosi_I), (R - rcosj_I)sini_I), rsinj_I), \forall i_I, j_I \in I.$$

Podemos ver este mapeo como viene en la figura 6.

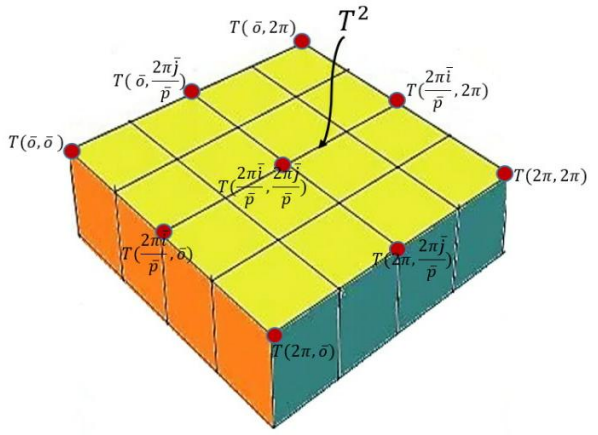


Figura 6: $\bar{K}$ visto como $k^n$.

**Construccion y Ejemplo del Cifrado Perturbado de Matsumoto-Imai 4.6.**

Sea $r$ un entero positivo pequeño, dado $(x_1, \ldots, x_n) \in k^n$ se debe de elegir al azar $r$ funciones lineales

$$z_i(x_1, \ldots, x_n) = \sum_{j=1}^{n} \alpha_{ji} x_j + \beta_i \in k,$$

en donde $\alpha_{ji}, \beta_i \in k$ para $i \in \{1, 2, \ldots, r\}$ y los terminos de grado uno deben de ser linealmente independientes. Habiendo definido las funciones $z_1(x_1, \ldots, x_n), \ldots, z_r(x_1, \ldots, x_n) \in k$ definimos una nueva función $Z : k^n \mapsto k^r$ tal que

$$Z(x_1, \ldots, x_n) = (z_1(x_1, \ldots, x_n), \ldots, z_r(x_1, \ldots, x_n)) =$$
$$(\sum_{j=1}^{n} \alpha_{j1} x_j + \beta_1, \ldots, \sum_{j=1}^{n} \alpha_{jr} x_j + \beta_r).$$

Para la siguiente parte primero eliga $r$ polinomios cuadráticos $f_1, \ldots, f_r$ al azar. Con estos polinomios definimos dos mapas:

1. $f : k^r \mapsto k^n$ tal que

$$f(z_1, \ldots, z_r) = (f_1(z_1, \ldots, z_r), )$$

# 5. Proceso

**Definicion 2.1**. La Criptografía de Variable Multiple es el estudio de los MPKCs donde la función trampa toma la forma de un polinomio cuadratico multivariable sobre un campo finito. En general la llave publica esta dada por un conjunto de polinomios cuadraticos: