Rainbow

Luis Cárcamo
Jesús Padilla
Fabián Osorio
Luis Sepúlveda

11 de octubre de 2019

1. Introducción

En este trabajo presentamos una implementación del esquema criptográfico de Rainbow. Gran parte de este trabajo está basado en el documento de la especificación presentada a la *NIST* por Ding [1]. Los aspectos teóricos tomados en cuenta están basados en la propuesta citada y en la presentación original hecha por Ding et al. [2]. Este esquema está basado en el *Unbalanced Oil and Vinegar Scheme*, presentado en [3].

Como aporte adicional a la propuesta enviada al *2nd round* de la NIST, se presentan aquí algunas optimizaciones en cuanto al cálculo de las llaves, sobre todo en lo relacionado a el cálculo de los productos matriciales.

2. Descripción general

El parámetro q define a $\mathbb{F} = \mathbb{F}_q$.

Solo se tendrán dos capas, esto implica el uso de los parámetros v_1, o_1 y o_2, donde $m = o_1 + o_2$ y $n = v_1 + m$ ($\implies m = n - v_1$). Donde n es el número de variables y m es el número de ecuaciones.

Dado que tenemos o_1 y o_2, entonces $u = 2$. Por lo tanto, tenemos

$$0 < v_1 < v_2 < v_3 = n.$$

y entonces

$$V_1 = \{1, \ldots, v_1\}, \qquad V_2 = \{1, \ldots, v_2\} \qquad \text{y} \qquad V_3 = \{1, \ldots, n\},$$

lo que a su vez implica

$$O_1 = \{v_1 + 1, \ldots, v_2\} \qquad O_2 = \{v_2 + 1, \ldots, n\}.$$

Donde $o_1 = |O_1| = v_2 - v_1$ y $o_2 = |O_2| = n - v_2$ y dado que conocemos o_1, o_2 y v_1, el valor de $v_2 = n - o_2 = o_1 + v_1$.

Además de la restricción a solo dos capas, se trabajará solo con mapas homogéneos. Dado que según [1], es la parte homogénea de mayor grado la que determina la complejidad de algún ataque directo, por lo que negligir los términos de menor orden al cuadrático no implica una reducción en la seguridad de este esquema.

Adicionalmente, para las operaciones aritméticas en esta implementación hacemos uso del campo $GF(2^8)$, usando el polinomio irreducible $x^8 + x^4 + x^3 + x + 1$.

Para las operaciones aritméticas sobre el campo nos apoyamos sobre la librería ***Bouncy Castle***. De esta librería usamos la API para los campos de Galois y las operaciones de suma y multiplicación sobre este. Todo lo demás fue implementado por el equipo, basados en –como se señaló antes– la especificación de referencia presentada en [1] y en [2].

3. Generación de llaves

Rainbow es un esquema asimétrico, por tanto, consta de dos llaves, siendo una privada y la otra pública. La llave privada es una 3-tupla que está compuesta por 2 mapas afines invertibles ($\mathcal{S}$ y $\mathcal{T}$) y un mapa central ($\mathcal{F}$). La llave pública $\mathcal{P}$ es igual a la composición del mapa afín $\mathcal{S}$ con el mapa afín $\mathcal{F}$ y el mapa afín $\mathcal{T}$.

- **Llave pública**: La llave pública es $\mathcal{P} = \mathcal{S} \circ \mathcal{F} \circ \mathcal{T}$.
- **Llave privada**: La llave privada es la 3-tupla $(\mathcal{S}, \mathcal{F}, \mathcal{T})$.

Donde

$$\mathcal{T} : \mathbb{F}^n \to \mathbb{F}^n,$$
$$\mathcal{F} : \mathbb{F}^n \to \mathbb{F}^m,$$
$$\mathcal{S} : \mathbb{F}^m \to \mathbb{F}^m.$$

Por lo tanto

$$\mathcal{P} : \mathbb{F}^n \to \mathbb{F}^m.$$

3.1. Mapa Central Cuadrático $\mathcal{F}$

$\mathcal{F}$ es el *mapa central* cuadrático, que tiene m polinomios multivariable $\left(f^{(v_1+1)}, \ldots, f^{(n)}\right)$. Cada uno de estos polinomios, que llamaremos $f^{(k)}$ es:

$$\begin{aligned} f^{(k)}(x_1, \ldots, x_n) = & \sum_{1 \le j \le v_l} \left(\sum_{1 \le i \le j} \alpha_{i,j}^{(k)} \cdot x_i \cdot x_j \right) \\ & + \sum_{v_l+1 \le i \le v_{l+1}} \left(\sum_{1 \le j \le v_l} \beta_{i,j}^{(k)} \cdot x_i \cdot x_j \right) + \sum_{1 \le i \le v_{l+1}} \gamma_i^{(k)} \cdot x_i + \delta^{(k)}, \end{aligned} \tag{1}$$

donde $\alpha_{i,j}$, $\beta_{i,j}$, γ_i y δ son elementos aleatorios del campo $\mathbb{F}$ (véase la sección 3.3).

Por otro lado, $l \in \{1, \ldots, u\}$ se refiere a el único entero tal que $k \in O_l$, es decir, l es el único entero tal que $v_l + 1 \le k \le v_{l+1}$. Sin embargo, dado que para efectos de la implementación a hacer se tomó el valor de $u = 2$, solo existen 2 posibles valores para l: 1 y 2. Por tanto, para cada $f^{(k)}$, el valor de l dependerá de cuál de las siguientes expresiones es válida:

$$\begin{aligned} l = 1: &\quad v_1 + 1 \le k \le v_2, \\ l = 2: &\quad v_2 + 1 \le k \le n. \end{aligned} \tag{2}$$

De (2) y (1) obtenemos las siguientes expresiones para $f^{(k)}$:

Para $v_1 + 1 \le k \le v_2$ ($\implies l = 1$):

$$\begin{aligned} f^{(k)}(x_1, \ldots, x_n) = & \sum_{1 \le j \le v_1} \left(\sum_{1 \le i \le j} \alpha_{i,j}^{(k)} \cdot x_i \cdot x_j \right) \\ & + \sum_{v_1+1 \le i \le v_2} \left(\sum_{1 \le j \le v_1} \beta_{i,j}^{(k)} \cdot x_i \cdot x_j \right) + \sum_{1 \le i \le v_2} \gamma_i^{(k)} \cdot x_i + \delta^{(k)}, \end{aligned} \tag{3}$$

y para $v_2 + 1 \le k \le n$ ($\implies l = 2$):

$$\begin{aligned} f^{(k)}(x_1, \ldots, x_n) = & \sum_{1 \le j \le v_2} \left(\sum_{1 \le i \le j} \alpha_{i,j}^{(k)} \cdot x_i \cdot x_j \right) \\ & + \sum_{v_2+1 \le i \le n} \left(\sum_{1 \le j \le v_2} \beta_{i,j}^{(k)} \cdot x_i \cdot x_j \right) + \sum_{1 \le i \le n} \gamma_i^{(k)} \cdot x_i + \delta^{(k)}, \end{aligned} \tag{4}$$

Además de esta restricción sobre l impuesta por el valor fijo de u, la restricción a trabajar únicamente con mapas homogéneos implica que estas ecuaciones quedarán de la siguiente forma:

Para $v_1 + 1 \leq k \leq v_2$ ($\implies l = 1$):

$$f^{(k)}(x_1, \ldots, x_n) = \sum_{1 \leq j \leq v_1} \left(\sum_{1 \leq i \leq j} \alpha_{i,j}^{(k)} \cdot x_i \cdot x_j \right) + \sum_{1 \leq i \leq v_1} \left(\sum_{v_1+1 \leq j \leq v_2} \beta_{i,j}^{(k)} \cdot x_i \cdot x_j \right), \quad (5)$$

y para $v_2 + 1 \leq k \leq n$ ($\implies l = 2$):

$$f^{(k)}(x_1, \ldots, x_n) = \sum_{1 \leq j \leq v_2} \left(\sum_{1 \leq i \leq j} \alpha_{i,j}^{(k)} \cdot x_i \cdot x_j \right) + \sum_{1 \leq i \leq v_2} \left(\sum_{v_2+1 \leq j \leq n} \beta_{i,j}^{(k)} \cdot x_i \cdot x_j \right). \quad (6)$$

Las ecuaciones (5) y (6) definen los m polinomios del *mapa central* homogéneo. Lo que hace que $\mathcal{F}$ esté compuesto por dos capas, determinadas cada uno por las ecuaciones citadas.

3.2. Representación de $\mathcal{S}$, $\mathcal{T}$, $\mathcal{F}$ y $\mathcal{P}$

La representación de $\mathcal{S}$, $\mathcal{T}$, y $\mathcal{F}$ y por tanto, de los polinomios, se hace por medio de matrices.

Para la el mapa afín $\mathcal{S}$, se asume que tiene la forma:

$$\mathcal{S} = \begin{pmatrix} \mathbf{I}_{o_1 \times o_1} & S'_{o_1 \times o_2} \\ \mathbf{0}_{o_2 \times o_1} & \mathbf{I}_{o_2 \times o_2} \end{pmatrix} \in \mathbb{F}^{m \times m} \quad (7)$$

En el caso del mapa afín $\mathcal{T}$, se asume que tiene la forma:

$$\mathcal{T} = \begin{pmatrix} \mathbf{I}_{v_1 \times v_1} & T^{(1)}_{v_1 \times o_1} & T^{(2)}_{v_1 \times o_2} \\ \mathbf{0}_{o_1 \times v_1} & \mathbf{I}_{o_1 \times o_1} & T^{(3)}_{o_1 \times o_2} \\ \mathbf{0}_{o_2 \times v_1} & \mathbf{0}_{o_2 \times o_1} & \mathbf{I}_{o_2 \times o_2} \end{pmatrix} \in \mathbb{F}^{n \times n} \quad (8)$$

Al restringir la forma de $\mathcal{S}$ y $\mathcal{T}$ a matrices de la forma triangular superior, se asegura que su determinante sea diferente de cero y en este caso, que sea igual a 1, asegurando así la invertibilidad de estas matrices, y por tanto, de los mapas afines, reduciendo así la complejidad computacional del algoritmo al evitar realizar la comprobación de su invertibilidad.

Para el caso del mapa central $\mathcal{F}$, se sabe que este consta de m polinomios $f^{(i)}$, $v_1 + 1 \leq i \leq n$, definidos cada uno por (5) para $v_1 + 1 \leq i \leq v_2$ y por (6) para $v_2 + 1 \leq i \leq n$.

Para los polinomios de la capa $l = 1$, es decir aquellos $f^{(i)}$ con $v_1 + 1 \leq i \leq v_2$, partiendo de la ecuación (5) que los define, se obtiene que tienen la forma:

$$f^{(i)} = \begin{pmatrix} F_1^{(i)} & F_2^{(i)} & \mathbf{0}_{v_1 \times o_2} \\ \mathbf{0}_{o_1 \times v_1} & \mathbf{0}_{o_1 \times v_1} & \mathbf{0}_{o_1 \times v_2} \\ \mathbf{0}_{o_2 \times v_1} & \mathbf{0}_{o_2 \times v_1} & \mathbf{0}_{o_2 \times v_2} \end{pmatrix}, \tag{9}$$

donde $F_1^{(i)} \in \mathbb{F}^{v_1 \times v_1}$, además, esta es una matriz triangular superior, y $F_2^{(i)} \in \mathbb{F}^{v_1 \times o_1}$. Los elementos de $F_1^{(i)}$ corresponden a los valores de los coeficientes α y los elementos de la submatriz $F_2^{(i)}$ corresponden a los coeficientes β del polinomio.

Por otro lado, para los polinomios de la capa $l = 2$, es decir aquellos $f^{(i)}$ con $v_2 + 1 \leq i \leq n$, partiendo de la ecuación (6) que los define, se obtiene que tienen la forma:

$$f^{(i)} = \begin{pmatrix} F_1^{(i)} & F_2^{(i)} & F_3^{(i)} \\ \mathbf{0}_{o_1 \times v_1} & F_5^{(i)} & F_6^{(i)} \\ \mathbf{0}_{o_2 \times v_1} & \mathbf{0}_{o_2 \times v_1} & \mathbf{0}_{o_2 \times v_2} \end{pmatrix}, \tag{10}$$

donde $F_1^{(i)} \in \mathbb{F}^{v_1 \times v_1}$,$F_2^{(i)} \in \mathbb{F}^{v_1 \times o_1}$, $F_3^{(i)} \in \mathbb{F}^{v_1 \times o_2}$, $F_5^{(i)} \in \mathbb{F}^{o_1 \times o_1}$ y $F_6^{(i)} \in \mathbb{F}^{o_1 \times o_2}$. Donde $F_1^{(i)}$ y $F_5^{(i)}$ son matrices de la forma triangular superior. Los elementos de $F_1^{(i)}$, $F_2^{(i)}$ y $F_5^{i)}$ corresponden a los valores de los coeficientes α y los elementos de la submatriz $F_3^{(i)}$ y $F_6^{(i)}$ corresponden a los coeficientes β del polinomio.

De modo que la representación de $\mathcal{F}$ se subdividirá en dos capas, $l = 1$ y $l = 2$, cada una de las cuales tendrá o_1 y o_2 (para un total de m) polinomios respectivamente, siendo estos polinimios representados como matrices, que a su vez están compuestas por submatrices, siendo la forma de las matrices para los polinomios de la capa $l = 1$ mostrada en (9) y para los polinomios de la capa $l = 2$ de la forma (10).

La representación de la llave pública $\mathcal{P}$ se hace mediante una 2-tupla de matrices MP_1 y MP_2. Estas matrices a su vez se calculan por medio de unas matrices $MQ1$ y $MQ2$, que contienen los coeficientes de los polinomios de las capas uno y dos, respectivamente. Más específicamente, las ecuaciones para las dos matrices que conforman la llave públicas son las siguientes:

$$\begin{aligned} MP1 &= MQ1 + S' \cdot MQ2, \\ MP2 &= MQ2. \end{aligned} \tag{11}$$

En la sección 3.4.2 se dan los detalles de la obtención de las matrices $MQ1$ y $MQ2$.

3.3. Generación de los elementos aleatorios

La matrices $S' \in \mathbb{F}^{o_1 \times o_2}$, $T^{(1)} \in \mathbb{F}^{v_1 \times o_1}$, $T^{(2)} \in \mathbb{F}^{v_1 \times o_2}$ y $T^{(3)} \in \mathbb{F}^{o_2 \times o_2}$, se generan aleatoriamente. Esto se hace seleccionando una semilla de 256 bits $\mathbf{s}_{\text{priv}}$ que por medio de un PRNG es usada para generar los elementos de estas matrices, que claramente deben estar en $\mathbb{F}$.

Con esta semilla ($\mathbf{s}_{\text{priv}}$) también se generan los coeficientes distintos a cero (α, β) del *mapa central* $\mathcal{F}$. Es importante anotar que en la implementación propuesta todos los elementos aleatorios generados son diferentes de cero.

3.4. Generación de llaves en Rainbow

En el Algoritmo 1 se especifica de manera general la generación de las llaves pública y privada en Rainbow.

Algorithm 1: Algoritmo de Generación de llaves de Rainbow

Entrada : $q,\ v_1,\ o_1,\ o_2$
Salida : $(s_k,\ p_k)$

$s_{\mathbf{p}} \leftarrow \text{SEED}(256)$
$S' \leftarrow \text{MATRIX}(s_{\mathbf{p}}, o_1, o_2)$
$\mathcal{S} \leftarrow \text{CreateS}(S', o_1, o_2)$
$T^{(1)} \leftarrow \text{MATRIX}(s_{\mathbf{p}}, v_1, o_1)$
$T^{(2)} \leftarrow \text{MATRIX}(s_{\mathbf{p}}, v_1, o_2)$
$T^{(3)} \leftarrow \text{MATRIX}(s_{\mathbf{p}}, o_1, o_2)$
$\mathcal{T} \leftarrow \text{CreateT}(T^{(1)}, T^{(2)}, T^{(3)}, v_1, o_1, o_2)$
$\mathcal{F} \leftarrow \text{RainbowMap}(s_{\mathbf{p}}, q, v_1, o_1, o_2)$
$\mathcal{P} \leftarrow \mathcal{S} \circ \mathcal{F} \circ \mathcal{T}$
$s_k \leftarrow (\mathcal{S}, \mathcal{F}, \mathcal{T})$
$pk \leftarrow \mathcal{P}$
return $(s_k,\ p_k)$

- La función SEED crea una semilla de la cantidad de bits indicada.
- La función Matrix(n, n) crea una matriz aleatoria **invertible** $M \in \mathbb{F}^{n \times n}$.
- La función RainbowMap crea el mapa central, representado como m matrices de $n \times n$.

- La función CreateS retorna un mapa afín basado en la ecuación (7).
- La función CreateT retorna un mapa afín basado en la ecuación (8).

Una vez establecido este algoritmo (visto de manera general), sin ninguna especificación sobre la implementación del mismo, procedemos a especificar cómo se realizará el cálculo del *mapa central* y de las llaves pública y privada.

3.4.1. Llave privada

La generación de la llave privada se resume entonces al a creación de 3 matrices T_1, T_2 y T_3 para la definición del mapa afín $\mathcal{T}$, de una matriz S' para el mapa afín $\mathcal{T}$ y de la creación de las 2 capas y sus respectivos polinomios, es decir, de la creación de las submatrices de cada polinomio. Todas estas matrices antes señaladas se generan de manera aleatoria haciendo uso de la semilla de 256 bits.

De modo que en resumen, la creación de la llave privada se resume en la creación de matrices aleatorias a partir de la semilla de 256 bits. Para los o_1 polinomios de la capa 1, se crean las submatrices F indicadas en la ecuación (9). Recíprocamente, para los o_2 polinomios de la capa 2, se crean las submatrices indicadas en la ecuación (10).

En la Tabla 1 se muestran las matrices que se deben crear en la generación de la llave privada. Todas estas matrices son creadas aleatoriamente. Las matrices F son distintas para cada polinomio y en esta tabla se omite el índice que indica el polinomio al que pertenecen. Debe tenerse en cuenta que las matrices F_1 y F_5 son de la forma triangular superior.

Matriz	Dimensiones	Cantidad
T_1	$v_1 \times o_1$	1
T_2	$v_1 \times o_2$	1
T_3	$o_1 \times o_2$	1
S'	$o_1 \times o_2$	1
F_1	$v_1 \times v_1$	m
F_2	$v_1 \times o_1$	m
F_3	$v_1 \times o_2$	o_2
F_5.	$o_1 \times o_1$	o_2
F_6	$o_1 \times o_2$	o_2

Cuadro 1: Matrices creadas en la generación de llave privada.

3.4.2. Llave pública

Ahora, se hace necesario hallar la llave pública $\mathcal{P}$, esto es:

$$\mathcal{P} = \mathcal{S} \circ \mathcal{F} \circ \mathcal{T} \tag{12}$$

De la ecuación (12), definimos un nuevo mapa $\mathcal{Q} = \mathcal{F} \circ \mathcal{T}$. Este mapa consta de m matrices $Q^{(i)}$, $i = v_i + 1, \ldots, n$, donde $Q^{(i)} = T^T \cdot F^{(i)} \cdot T$.

Cada una de estas matrices $Q^{(i)}$ tiene la forma

$$Q^{(i)} = \begin{pmatrix} Q^{(i,1)}_{v_1 \times v_1} & Q^{(i,2)}_{v_1 \times o_1} & Q^{(i,3)}_{v_1 \times o_2} \\ \mathbf{0}_{o_1 \times v_1} & Q^{(i,5)}_{o_1 \times o_1} & Q^{(i,6)}_{o_1 \times o_2} \\ \mathbf{0}_{o_2 \times v_1} & \mathbf{0}_{o_2 \times o_1} & Q^{(i,9)}_{o_2 \times o_2} \end{pmatrix}. \tag{13}$$

Donde $Q^{(i,1)}$, $Q^{(i,5)}$ y $Q^{(i,9)}$ son matrices de la forma triangular superior y por tanto, dada la estructura de $Q^{(i)}$, mostrada en (13), $Q^{(i)}$ será también una matriz triangular superior. La definición inicial de estas submatrices es tomada de [1] y aquí presentamos algunas mejoras en el cálculo de estas.

A continuación, definimos para la capa $l = 1$ cada una de estas submatrices de la siguiente forma:

$$\begin{aligned}
Q^{(i,1)} &= F_1^{(i)} \\
Q^{(i,2)} &= \left(F_1^{(i)} + \left[F_1^{(i)}\right]^T\right) \cdot T_1 + F_2^{(i)} \\
Q^{(i,3)} &= \left(F_1^{(i)} + \left[F_1^{(i)}\right]^T\right) \cdot T_2 + F_2^{(i)} \cdot T_3 \\
Q^{(i,5)} &= UT\left(T_1^T \cdot F_1^{(i)} \cdot T_1 + T_1^T \cdot F_2^{(i)}\right) \\
Q^{(i,6)} &= T_1^T \cdot \left(F_1^{(i)} + \left[F_1^{(i)}\right]^T\right) \cdot T_2 + T_1^T \cdot F_2^{(i)} \cdot T_3 + \left[F_2^{(i)}\right]^T \cdot T_2 \\
Q^{(i,9)} &= UT\left(T_2^T \cdot F_1^{(i)} \cdot T_2 + T_2^T \cdot F_2^{(i)} \cdot T_3\right)
\end{aligned}$$

Definiendo nuevas matrices para evitar el re-cálculo de producto de matrices, tenemos:

$$\begin{aligned}
A^{(i)} &= F_1^{(i)} + (F_1^{(i)})^T = \left[A^{(i)}\right]^T \\
B^{(i)} &= F_2^{(i)} \cdot T_3 \\
C^{(i)} &= A^{(i)} \cdot T_1 \\
D^{(i)} &= C^{(i)} + F_2^{(i)}
\end{aligned} \tag{14}$$

De modo que las ecuaciones para las submatrices de $Q^{(i)}$ en la capa uno quedan definidas de la siguiente forma:

$$\begin{aligned} Q^{(i,1)} &= F_1^{(i)} \\ Q^{(i,2)} &= D^{(i)} \\ Q^{(i,3)} &= A^{(i)} \cdot T_2 + B^{(i)} \\ Q^{(i,5)} &= UT\left(T_1^T \cdot \left(F_1^{(i)} \cdot T_1 + F_2^{(i)}\right)\right) \\ Q^{(i,6)} &= \left[D^{(i)}\right]^T \cdot T_2 + T_1^T \cdot B^{(i)} \\ Q^{(i,9)} &= UT\left(T_2^T \cdot \left(F_1^{(i)} \cdot T_2 + B^{(i)}\right)\right) \end{aligned} \tag{15}$$

Nótese que $A^{(i)} = \left[A^{(i)}\right]^T$. Entonces:

$$\begin{aligned} C^{(i)} &= A^{(i)} \cdot T_1 = \left[A^{(i)}\right]^T \cdot T_1 \\ \left[C^{(i)}\right]^T &= \left[\left[A^{(i)}\right]^T \cdot T_1\right]^T = T_1^T \cdot A^{(i)}. \end{aligned}$$

Adicional a esto,

$$\begin{aligned} Q^{(i,6)} &= T_1^T \cdot \left(F_1^{(i)} + \left[F_1^{(i)}\right]^T\right) \cdot T_2 + T_1^T \cdot F_2^{(i)} \cdot T_3 + \left[F_2^{(i)}\right]^T \cdot T_2 \\ &= T_1^T \cdot A \cdot T_2 + T_1^T \cdot B^{(i)} + \left[F_2^{(i)}\right]^T \cdot T_2 = \left(T_1^T \cdot A + \left[F_2^{(i)}\right]^T\right) \cdot T_2 + T_1^T \cdot B^{(i)} \\ &= \left(\left[C^{(i)}\right]^T + \left[F_2^{(i)}\right]^T\right) \cdot T_2 + T_1^T \cdot B^{(i)} = \left(C^{(i)} + F_2^{(i)}\right)^T \cdot T_2 + T_1^T \cdot B^{(i)} \\ Q^{(i,6)} &= \left[D^{(i)}\right]^T \cdot T_2 + T_1^T \cdot B^{(i)}. \end{aligned}$$

Las demás ecuaciones para los $Q^{(i,j)}$ surgen por simple reemplazo. La función UT recibe como parámetro una matriz cuadrada y la convierte a la forma triangular superior.

De esta forma se reduce la complejidad computacional en el cálculo de las submatrices de $Q^{(i)}$ en la capa 1.

Para la capa $l = 2$, también se definen estas submatrices y se procede de manera similar para optimizar la cantidad de multiplicaciones necesarias.

$$
\begin{aligned}
Q^{(i,1)} &= F_1^{(i)} \\
Q^{(i,2)} &= \left(F_1^{(i)} + \left[F_1^{(i)}\right]^T\right) \cdot T_1 + F_2^{(i)} \\
Q^{(i,3)} &= \left(F_1^{(i)} + \left[F_1^{(i)}\right]^T\right) \cdot T_2 + F_2^{(i)} \cdot T_3 + F_3^{(i)} \\
Q^{(i,5)} &= UT\left(T_1^T \cdot F_1^{(i)} \cdot T_1 + T_1^T \cdot F_2^{(i)} + F_5^{(i)}\right) \\
Q^{(i,6)} &= T_1^T \cdot \left(F_1^{(i)} + \left[F_1^{(i)}\right]^T\right) \cdot T_2 + T_1^T \cdot F_2^{(i)} \cdot T_3 + T_1^T \cdot F_3^{(i)} \\
&\quad + \left[F_2^{(i)}\right]^T \cdot T_2 + \left(F_5^{(i)} + \left[F_5^{(i)}\right]^T\right) \cdot T_3 + F_6^{(i)} \\
Q^{(i,9)} &= UT\left(T_2^T \cdot F_1^{(i)} \cdot T_2 + T_2^T \cdot F_2^{(i)} \cdot T_3 + T_3^T \cdot F_5^{(i)} \cdot T_3 + T_2^T \cdot F_3^{(i)} + T_3^T \cdot F_6^{(i)}\right)
\end{aligned}
$$

Haciendo uso de las matrices previamente definidas en (14), y además, aplicando las propiedades asociativas y distributivas de las matrices, definimos una nueva matriz $E^{(i)}$ y reescribimos las ecuaciones para las submatrices de $Q^{(i)}$ para los polinomios de la capa 2, reduciendo así la cantidad de cómputo necesaria para su cálculo.

$$
\begin{aligned}
Q^{(i,1)} &= F_1^{(i)}, \\
Q^{(i,2)} &= D^{(i)}, \\
Q^{(i,3)} &= G^{(i)}, \\
Q^{(i,5)} &= UT\left(T_1^T \cdot \left(F_1^{(i)} \cdot T_1 + F_2^{(i)}\right) + F_5^{(i)}\right), \\
Q^{(i,6)} &= T_1^T \cdot G^{(i)} + \left[F_2^{(i)}\right]^T \cdot T_2 + \left(F_5^{(i)} + \left[F_5^{(i)}\right]^T\right) \cdot T_3 + F_6^{(i)}, \\
Q^{(i,9)} &= UT\left(T_2^T \cdot \left(F_1^{(i)} \cdot T_2 + E^{(i)}\right) + T_3^T \cdot \left(F_5^{(i)} \cdot T_3 + F_6^{(i)}\right)\right),
\end{aligned}
\tag{16}
$$

donde

$$
E^{(i)} = B^{(i)} + F_3^{(i)}, \qquad G^{(i)} = A^{(i)} \cdot T_2 + E^{(i)}.
$$

Nuevamente, estas expresiones surgen por un simple reemplazo o aplicación de propiedad asociativa, a excepción de la ecuación para $Q^{(i,6)}$ que, a pesar de ser obtenida mediante las mismas aplicaciones, requiere un par de pasos más. Estos pasos

son mostrados a continuación.

$$\begin{aligned}
Q^{(i,6)} &= T_1^T \cdot \left(F_1^{(i)} + \left[F_1^{(i)}\right]^T\right) \cdot T_2 + T_1^T \cdot F_2^{(i)} \cdot T_3 + T_1^T \cdot F_3^{(i)} \\
&+ \left[F_2^{(i)}\right]^T \cdot T_2 + \left(F_5^{(i)} + \left[F_5^{(i)}\right]^T\right) \cdot T_3 + F_6^{(i)} \\
&= T_1^T \cdot \left(A^{(i)} \cdot T_2 + B^{(i)} + F_3^{(i)}\right) + \left[F_2^{(i)}\right]^T \cdot T_2 + \left(F_5^{(i)} + \left[F_5^{(i)}\right]^T\right) \cdot T_3 + F_6^{(i)} \\
&= T_1^T \cdot \left(A^{(i)} \cdot T_2 + E^{(i)}\right) + \left[F_2^{(i)}\right]^T \cdot T_2 + \left(F_5^{(i)} + \left[F_5^{(i)}\right]^T\right) \cdot T_3 + F_6^{(i)} \\
&= T_1^T \cdot G^{(i)} + \left[F_2^{(i)}\right]^T \cdot T_2 + \left(F_5^{(i)} + \left[F_5^{(i)}\right]^T\right) \cdot T_3 + F_6^{(i)}.
\end{aligned}$$

Una vez que las matrices definidas en las ecuaciones (15) y (16) hayan sido calculadas para cada uno de los m polinomios, se procede a realizar el cálculo de las matrices $MQ1$ y $MQ2$ y a partir de estas matrices y S', se hallan las matrices que conforman la llave pública, por medio de las ecuaciones definidas en (11).

El llenado de las matrices $MQ1$ y $MQ2$ es hecho por medio de las matrices Q de las capas uno y dos, respectivamente. Y siguen el mismo procedimiento, insertando los elementos de la matrices $Q^{(i)}$, $i = v_1 + 1, \ldots, n$ en la fila $i - v_1$ de la matriz $MQ1$ para $v_1 + 1 \leq i \leq v_2$ y en la matriz $MQ2$ para $v_2 + 1 \leq i \leq n$. Es decir, los valores de las matrices $Q^{(i)}$ asociados a la primera capa van en $MQ1$ y los asociados con la segunda capa van en la matriz $MQ2$.

Dicho esto, para cada fila de las matrices (sea $MQ1$ o $MQ2$) se procede del siguiente modo:

1. Insertar los elementos de $Q_1^{(i)}||Q_2^{(i)}$ en la fila. Tenga en cuenta que $Q_1^{(i)}$ es una matriz triangular superior y que de esta solo se tomarán los elementos de la triangular superior.

2. Los siguientes elementos de la matriz corresponden con los elementos de $Q_3^{(i)}$.

3. Los siguientes elementos de la fila provienen de insertar los elementos de $Q_5^{(i)}||Q_6^{(i)}$. Nuevamente, teniendo en cuenta que $Q_5^{(i)}$ es una matriz triangular superior.

4. Finalmente, las posiciones restantes se llenan con los elementos de la triangular superior de $Q_9^{(i)}$.

Cada recorrido por las matrices se hace de izquierda a derecha y de arriba hacia abajo.

Una vez calculadas las matrices $MQ1$ y $MQ2$ se procede a calcular las matrices $MP1$ y $MP2$, aplicando las ecuaciones (11). De modo que a través de este procedimiento se halla la llave pública de este esquema. En el Algoritmo 2 se describe la generación de la llave pública.

Algorithm 2: Algoritmo de generación de la llave pública

Entrada : $Q^{(i)},\ v_1 + 1 \leq i \leq n;\ S'$.
Salida : $(MP1,\ MP2)$.

para $i \leftarrow v_1 + 1$ **hasta** v_2 ▷ *Capa 1*
  Insertar los elementos de $Q_1^{(i)}||Q_2^{(i)}$ en la fila $i - v_1$ de $MQ1$.
  Insertar los elementos de $Q_3^{(i)}$ en las siguientes posiciones de la fila $i - v_1$ de $MQ1$.
  Insertar los elementos de $Q_5^{(i)}||Q_6^{(i)}$ en las siguientes posiciones de fila $i - v_1$ de $MQ1$.
  Insertar los elementos de $Q_9^{(i)}$ en las siguientes posiciones de la fila $i - v_1$ de $MQ1$.
fin_para
para $i \leftarrow v_2 + 1$ **hasta** n ▷ *Capa 2*
  Insertar los elementos de $Q_1^{(i)}||Q_2^{(i)}$ en la fila $i - v_2$ de $MQ2$.
  Insertar los elementos de $Q_3^{(i)}$ en las siguientes posiciones de la fila $i - v_2$ de $MQ2$.
  Insertar los elementos de $Q_5^{(i)}||Q_6^{(i)}$ en las siguientes posiciones de fila $i - v_2$ de $MQ2$.
  Insertar los elementos de $Q_9^{(i)}$ en las siguientes posiciones de la fila $i - v_2$ de $MQ2$.
fin_para
$MP1 \leftarrow MQ1 + S' \cdot MQ2$.
$MP1 \leftarrow MQ2$.
return $(MP1,\ MP2)$

Referencias

[1] Jintai Ding. «Rainbow». En: Post-Quantum Cryptography. Round 2 Submissions. Págs. 1-45.

[2] Jintai Ding y Dieter Schmidt. «Rainbow, a New Multivariable Polynomial Signature Scheme». En: *Applied Cryptography and Network Security*. Ed. por John Ioannidis, Angelos Keromytis y Moti Yung. Berlin, Heidelberg: Springer Berlin Heidelberg, 2005, págs. 164-175. ISBN: 978-3-540-31542-1.

[3] Aviad Kipnis, Jacques Patarin y Louis Goubin. «Unbalanced Oil and Vinegar Signature Schemes». En: *Advances in Cryptology — EUROCRYPT '99*. Ed. por Jacques Stern. Berlin, Heidelberg: Springer Berlin Heidelberg, 1999, págs. 206-222. ISBN: 978-3-540-48910-8.