Generación de las claves

1. **Generamos la clave privada:** La clave privada consiste en la sección de la superficie. Esta sección se compone de dos polinomios $u_x(t)$ y $u_y(t)$ de la forma siguiente:

$$\begin{aligned} u_x(t) &= a_3t^3 + a_2t^2 + a_1t + a_0 \\ u_y(t) &= b_3t^3 + b_2t^2 + b_1t + b_0 \end{aligned}$$

   El grado de estos polinomios lo fijamos como $\deg u_x(t) = \deg u_y(t) = 3$. Además los coeficientes son generados de manera aleatoria utilizando la librería estándar de C++ Mersenne-twister.

2. **Definimos el conjunto** Λ_X: Para formar la clave pública, es decir, la superficie, necesitaremos un conjunto de polinomios generados de manera aleatoria y cuyos grados los definimos a través del conjunto Λ_X:

$$\Lambda_X = \{(i,j) \in \mathbb{N}^2 : i = 1, \ldots, I, j = 1, \ldots, J\}$$

   Es decir, podemos, por ejemplo, definir a Λ_X como

$$\begin{aligned} (0,0) &\quad l_{00} = 1 \\ (1,0) &\quad l_{10} = 2 \\ (0,2) &\quad l_{02} = 4 \\ (3,0) &\quad l_{30} = 3 \\ (2,2) &\quad l_{22} = 3 \\ (4,4) &\quad l_{44} = 6 \end{aligned}$$

3. **Generamos los polinomios aleatorios** $c_{ij}(t)$: definimos polinomios de la forma $c_{ij}(t)$, donde además los valores l_{ij} representan el grado del polinomio correspondiente.

   Los pares ordenados (i,j) en Λ_X serán las potencias de x y y respectivamente cuando formemos la superficie.

4. **Sustitución de la sección en la superficie**: Utilizando los polinomios $c_{ij}(t)$ generados en el paso previo, vamos a formar la superficie, la cual tendrá la forma:

$$X(x,y,t) = \sum_{(i,j)\in\Lambda_X} c_{ij}(t)x^iy^j$$

   Esto es, si continuamos con el ejemplo previo de Λ_X, la superficie tendrá la forma:

$$X(x,y,t) = c_{00}(t) + c_{10}(t)x + c_{02}(t)y^2 + c_{30}(t)x^3 + c_{22}(t)x^2y^2 + c_{44}(t)x^4y^4$$

   aquí, cada polinomio $c_{ij}(t)$ tiene el grado correspondiente l_{ij} definido arriba.

   Para que la sección forme parte de la superficie debemos hacer la sustitución de los polinomios $u_x(t)$ y $u_y(t)$ en $X(x,y,t)$.

$$D = X(u_x(t), u_y(t), t)$$

   De esta manera garantizamos que la sección esté totalmente contenida en la superficie.

5. **Definimos la Clave pública**: Finalmente escribimos la clave pública como polinomio de tres variables utilizando la sustitución previa de D en $X(x, y, t)$, esto es, la clave pública tendrá la forma

$$X(x, y, t) = \sum_{(i,j)\in\Lambda_X} c_{ij}(t)x^i y^j - D$$

Ejemplo 1 *Para ilustrar este procedimiento, veamos un ejemplo sencillo con valores manejables:*

1. ***Generamos la clave privada:***

$$\begin{aligned} u_x(t) &= 2t^2 + t + 1 \\ u_y(t) &= t^2 + 1 \end{aligned}$$

2. ***Definimos el conjunto*** Λ_X*:*

$$\begin{aligned} (0,0) &\quad l_{00} = 1 \\ (1,1) &\quad l_{11} = 2 \\ (1,2) &\quad l_{12} = 2 \end{aligned}$$

3. ***Generamos los polinomios aleatorios*** $c_{ij}(t)$*:*

$$\begin{aligned} c_{00}(t) &= t + 2 \\ c_{11}(t) &= 3t^2 + 2t + 1 \\ c_{12}(t) &= 4t^2 + 3t + 3 \end{aligned}$$

4. ***Sustitución de la sección en la superficie:***

$$\begin{aligned} D &= X(u_x(t), u_y(t), t) \\ &= c_{00}(t) + c_{11}(t)xy + c_{12}(2)(t)xy^2 \\ &= (t+2) + (3t^2 + 2t + 1)xy + (4t^2 + 3t + 3)xy^2 \\ &= (t+2) + (3t^2 + 2t + 1)(2t^2 + t + 1)(t^2 + 1) + (4t^2 + 3t + 3)(2t^2 + t + 1)(t^2 + 1)^2 \\ &= (t+2) + (6t^4 + 7t^3 + 7t^2 + 3t + 1)(t^2 + 1) + (8t^4 + 10t^3 + 13t^2 + 6t + 3)(t^4 + 2t^2 + 1) \\ &= 8t^8 + 10t^7 + 35t^6 + 33t^5 + 50t^4 + 32t^3 + 27t^2 + 10t + 6 \end{aligned}$$

5. ***Definimos la Clave pública:***

$$\begin{aligned} X(x, y, t) &= c_{00}(t) + c_{11}(t)xy + c_{12}(2)(t)xy^2 - D \\ &= (t+2) + (3t^2 + 2t + 1)xy + (4t^2 + 3t + 3)xy^2 - (8t^8 + 10t^7 + 35t^6 + 33t^5 + 50t^4 + 32t^3 + 27t^2 + 10t + 6) \\ &= 3t^2xy + 2txy + xy + 4t^2xy^2 + 3txy^2 + 3xy^2 - (8t^8 + 10t^7 + 35t^6 + 33t^5 + 50t^4 + 32t^3 + 27t^2 + 9t + 4) \end{aligned}$$