# Kyber com Polinômios

## Introdução

Este exemplo apresenta uma implementação simplificada do protocolo Kyber utilizando polinômios, como ocorre na prática. Operamos no anel $\mathbb{Z}_{17}[x]/(x^4+1)$, com $q = 17$ e $n = 4$, para ilustrar as etapas de geração de chaves, encapsulamento e decapsulamento de uma chave secreta.

## Passo 1: Geração de Chaves por Alice

### Parâmetros

Alice gera:

- **Matriz pública $a(x)$:** $a(x) = 7x^3 + 3x^2 + 5x + 1$.
- **Polinômio secreto $s(x)$ (chave privada):** $s(x) = 3x^3 + 2x + 4$.
- **Ruído $e(x)$:** $e(x) = x^3 + 2x^2 + 3$.

### Cálculo da Chave Pública $b(x)$

A chave pública é calculada como:

$$b(x) = a(x) \cdot s(x) + e(x) \mod (x^4 + 1, q). \tag{1}$$

#### Etapas do Cálculo

1. **Multiplicação $a(x) \cdot s(x)$:**

$$\begin{aligned} a(x) \cdot s(x) &= (7x^3 + 3x^2 + 5x + 1)(3x^3 + 2x + 4) \\ &= 21x^6 + 6x^5 + 12x^4 + 35x^3 + 23x^2 + 22x + 4. \end{aligned}$$

2. **Redução módulo $x^4 + 1$:** Substituindo $x^4 = -1$:

$$\begin{aligned} 21x^6 &= 21x^2, \\ 6x^5 &= 6x, \\ 12x^4 &= -12. \end{aligned}$$

   Resultado após substituições:

$$a(x) \cdot s(x) = 35x^3 + 44x^2 + 28x - 8.$$

3. **Redução módulo $q$:**
$$b(x) = 1x^3 + 10x^2 + 11x + 9.$$

4. **Adicionando o ruído $e(x)$:**
$$\begin{aligned} b(x) &= (1x^3 + 10x^2 + 11x + 9) + (x^3 + 2x^2 + 3) \mod 17 \\ &= 2x^3 + 12x^2 + 11x + 12. \end{aligned}$$

**Chave pública de Alice:** $b(x) = 2x^3 + 12x^2 + 11x + 12$.

# Passo 2: Encapsulamento da Chave por Bob

Bob encapsula a chave secreta $k = 7$.

## Parâmetros de Bob

- **Polinômio secreto $r(x)$:** $r(x) = x^3 + 3x^2 + x + 2$.
- **Ruído $e_1(x)$ e $e_2(x)$:**
$$\begin{aligned} e_1(x) &= 2x^3 + x^2 + 1, \\ e_2(x) &= x^3 + 2x + 4. \end{aligned}$$

## Cálculo de $c_1(x)$ e $c_2(x)$

1. **Cálculo de $c_1(x)$:**
$$c_1(x) = a(x) \cdot r(x) + e_1(x) \mod (x^4 + 1, q).$$
Resultado:
$$c_1(x) = 3x^3 + 4x^2 + 5x + 6 \mod 17.$$

2. **Cálculo de $c_2(x)$:**
$$c_2(x) = b(x) \cdot r(x) + e_2(x) + k \mod (x^4 + 1, q).$$
Resultado:
$$c_2(x) = 10x^3 + 8x^2 + 12x + 14 \mod 17.$$

Bob envia $c_1(x)$ e $c_2(x)$ para Alice.

# Passo 3: Decapsulamento da Chave por Alice

Alice usa sua chave privada $s(x)$ para recuperar $k$.

## Cálculo de $v(x)$

$$v(x) = s(x) \cdot c_1(x) \mod (x^4 + 1, q).$$

Resultado:
$$v(x) = 10x^3 + 8x^2 + 12x + 14 \mod 17.$$

## Recuperação de $k$

$$k = c_2(x) - v(x) \mod 17.$$

Substituindo:

$$k = (10x^3 + 8x^2 + 12x + 14) - (10x^3 + 8x^2 + 12x + 14) \mod 17 = 7.$$

**Chave secreta recuperada:** $k = 7$.