Assinatura Digital com Dilithium

Introdução

O esquema de assinatura digital Dilithium é um dos padrões de criptografia pós-quântica aprovados pelo NIST. Ele utiliza matemática baseada em *lattices* (redes geométricas) para prover segurança contra ataques quânticos. Este exemplo ilustra as fases do protocolo com cálculos simplificados.

Parâmetros

- $q = 17$: Módulo para operações aritméticas.
- Vetor público A: Uma matriz 2×2 conhecida por todos:

$$A = \begin{bmatrix} 3 & 5 \\ 7 & 4 \end{bmatrix} \tag{1}$$

- Vetores secretos (chave privada de Alice):

$$s_1 = [2, 3],$$
$$s_2 = [1, 4].$$

- Função hash simplificada:

$$\text{Hash}(m) = [1, 2], \tag{2}$$

  onde m é a mensagem a ser assinada.

Fase 1: Geração de Chaves

Alice precisa gerar sua chave pública e privada.

Cálculo da chave pública (t)

A chave pública é calculada como:

$$t = A \cdot s_1 + s_2 \pmod{q} \tag{3}$$

Multiplicando a matriz A pelo vetor s_1:

$$A \cdot s_1 = \begin{bmatrix} 3 & 5 \\ 7 & 4 \end{bmatrix} \cdot \begin{bmatrix} 2 \\ 3 \end{bmatrix} = \begin{bmatrix} (3 \cdot 2 + 5 \cdot 3) \\ (7 \cdot 2 + 4 \cdot 3) \end{bmatrix} = \begin{bmatrix} 21 \\ 26 \end{bmatrix}. \tag{4}$$

Somando s_2 e aplicando o módulo q:

$$t = \begin{bmatrix} 21 \\ 26 \end{bmatrix} + \begin{bmatrix} 1 \\ 4 \end{bmatrix} \pmod{17} = \begin{bmatrix} 22 \\ 30 \end{bmatrix} \pmod{17} = \begin{bmatrix} 5 \\ 13 \end{bmatrix}. \tag{5}$$

Resultado

- **Chave pública (t):** $[5, 13]$.
- **Chave privada (s_1, s_2):** $[2, 3], [1, 4]$.

Fase 2: Assinatura da Mensagem

Alice deseja assinar a mensagem $m =$ "Hello".

Passo 1: Gerar vetor aleatório (y)

Alice escolhe um vetor aleatório:

$$y = [3, 2]. \tag{6}$$

Passo 2: Cálculo do valor intermediário (w)

O valor w é calculado como:

$$w = A \cdot y \pmod{q}. \tag{7}$$

Multiplicando:

$$A \cdot y = \begin{bmatrix} 3 & 5 \\ 7 & 4 \end{bmatrix} \cdot \begin{bmatrix} 3 \\ 2 \end{bmatrix} = \begin{bmatrix} (3 \cdot 3 + 5 \cdot 2) \\ (7 \cdot 3 + 4 \cdot 2) \end{bmatrix} = \begin{bmatrix} 19 \\ 29 \end{bmatrix}. \tag{8}$$

Aplicando o módulo q:

$$w = \begin{bmatrix} 19 \\ 29 \end{bmatrix} \pmod{17} = \begin{bmatrix} 2 \\ 12 \end{bmatrix}. \tag{9}$$

Passo 3: Calcular o hash da mensagem (c)

Alice calcula o hash:

$$c = \text{Hash}(w, m) = [1, 2]. \tag{10}$$

Passo 4: Cálculo da assinatura (z)

Alice calcula:

$$z = y + c \cdot s_1 \pmod{q}. \tag{11}$$

Multiplicando $c \cdot s_1$:

$$c \cdot s_1 = [1, 2] \cdot [2, 3] = [2, 6]. \tag{12}$$

Somando y e aplicando o módulo q:

$$z = [3, 2] + [2, 6] \pmod{17} = [5, 8]. \tag{13}$$

Resultado

A assinatura é:

- $z = [5, 8]$
- $c = [1, 2]$

Fase 3: Verificação da Assinatura

Bob verifica a assinatura (z, c) usando a chave pública t.

Passo 1: Recalcular w'

Bob calcula:

$$w' = A \cdot z - c \cdot t \pmod{q}. \tag{14}$$

Multiplicando $A \cdot z$:

$$A \cdot z = \begin{bmatrix} 3 & 5 \\ 7 & 4 \end{bmatrix} \cdot \begin{bmatrix} 5 \\ 8 \end{bmatrix} = \begin{bmatrix} (3 \cdot 5 + 5 \cdot 8) \\ (7 \cdot 5 + 4 \cdot 8) \end{bmatrix} = \begin{bmatrix} 55 \\ 71 \end{bmatrix}. \tag{15}$$

Aplicando o módulo q:

$$A \cdot z \pmod{17} = \begin{bmatrix} 55 \\ 71 \end{bmatrix} \pmod{17} = \begin{bmatrix} 4 \\ 3 \end{bmatrix}. \tag{16}$$

Calculando $c \cdot t$:

$$c \cdot t = [1, 2] \cdot [5, 13] = [5, 26]. \tag{17}$$

Aplicando o módulo q:

$$c \cdot t \pmod{17} = [5, 26] \pmod{17} = [5, 9]. \tag{18}$$

Subtraindo e aplicando o módulo q:

$$w' = \begin{bmatrix} 4 \\ 3 \end{bmatrix} - \begin{bmatrix} 5 \\ 9 \end{bmatrix} \pmod{17} = \begin{bmatrix} -1 \\ -6 \end{bmatrix} \pmod{17} = \begin{bmatrix} 16 \\ 11 \end{bmatrix}. \tag{19}$$

Passo 2: Comparar hashes

Bob calcula:

$$c' = \text{Hash}(w', m). \tag{20}$$

Se $c' = c$, a assinatura é válida.

Resultado

Como $c' = [1, 2]$, a assinatura é válida.