Assinatura Digital com SPHINCS+

Introdução

O esquema de assinatura digital SPHINCS+ é um dos padrões de criptografia pós-quântica aprovados pelo NIST. Ele utiliza *árvores de Merkle*, hashing e esquemas de retenção para prover segurança estatística e resistência a ataques quânticos. Este exemplo ilustra as fases do protocolo com cálculos simplificados.

Parâmetros

- **Tamanho da árvore de Merkle:** 3 níveis.
- **Folhas por árvore:** $2^2 = 4$ folhas.
- **Hash utilizado:** $H(x) = (x^2 + 1) \mod 17$.

Fase 1: Geração de Chaves

Passo 1: Geração das folhas

Alice gera 4 valores secretos (SK_i):

$$SK_1 = 2, \qquad SK_2 = 3, \qquad SK_3 = 4, \qquad SK_4 = 5.$$

Calcula os hashes das folhas ($PK_i = H(SK_i)$):

$$\begin{aligned} PK_1 = H(2) &= (2^2 + 1) \mod 17 = 5, \\ PK_2 = H(3) &= (3^2 + 1) \mod 17 = 10, \\ PK_3 = H(4) &= (4^2 + 1) \mod 17 = 0, \\ PK_4 = H(5) &= (5^2 + 1) \mod 17 = 9. \end{aligned}$$

As folhas da árvore de Merkle são:

$$[5, 10, 0, 9]. \tag{1}$$

Passo 2: Construção da árvore de Merkle

Alice combina os hashes das folhas para criar os nós intermediários e a raiz:

- **Primeiro nível:**

$$H_1 = H(5+10) = ((5+10)^2+1) \mod 17 = (15^2+1) \mod 17 = 6,$$
$$H_2 = H(0+9) = ((0+9)^2+1) \mod 17 = (9^2+1) \mod 17 = 14.$$

- **Raiz da árvore:**

$$\text{Raiz} = H(6+14) = ((6+14)^2+1) \mod 17 = (20^2+1) \mod 17 = 13. \quad (2)$$

Resultado

- **Chave privada (SK):** SK_1, SK_2, SK_3, SK_4.
- **Chave pública (PK):** Raiz da árvore: 13.

Fase 2: Assinatura da Mensagem

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

Passo 1: Gerar índice da folha

Alice calcula o índice da folha a partir do hash da mensagem:

$$\acute{}\text{ndice} = H(m) = (\text{"Hello"}^2+1) \mod 4 = (2^2+1) \mod 4 = 1. \quad (3)$$

Folha escolhida: $SK_2 = 3$.

Passo 2: Assinar a mensagem

Alice usa o valor secreto correspondente à folha ($SK_2 = 3$).

Passo 3: Construir a prova de autenticação

A prova inclui os hashes necessários para reconstruir a raiz:

- Hash irmão da folha: $PK_1 = 5$.
- Hash do nó superior: $H_2 = 14$.

Assinatura Final

A assinatura consiste em:

- $SK_2 = 3$.
- **Prova:** $[5, 14]$.

Fase 3: Verificação da Assinatura

Bob verifica a assinatura ($SK_2 = 3, \text{prova} = [5, 14]$) usando a chave pública PK.

Passo 1: Recalcular o hash da folha

Bob calcula:

$$PK_2 = H(SK_2) = (3^2 + 1) \mod 17 = 10. \tag{4}$$

Passo 2: Reconstruir a raiz

Bob combina PK_2 com o hash irmão ($PK_1 = 5$) para calcular o nó intermediário:

$$H_1 = H(PK_1 + PK_2) = H(5 + 10) = ((5 + 10)^2 + 1) \mod 17 = 6. \tag{5}$$

Combina H_1 com o hash do nó superior ($H_2 = 14$) para calcular a raiz:

$$\text{Raiz} = H(H_1 + H_2) = H(6 + 14) = ((6 + 14)^2 + 1) \mod 17 = 13. \tag{6}$$

Passo 3: Comparar raízes

Bob compara a raiz calculada (13) com a chave pública (13). Como as raízes coincidem, a assinatura é válida.