

# Otimização de desempenho do esquema de assinatura digital Winternitz

Gustavo Zambonin



Universidade Federal de Santa Catarina  
Departamento de Informática e Estatística

`gustavo.zambonin@grad.ufsc.br`

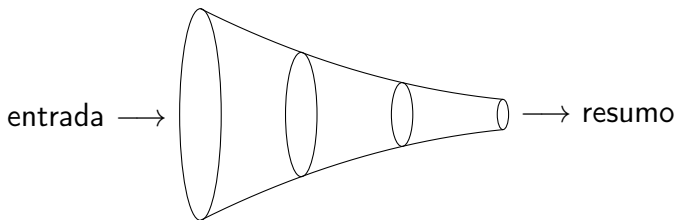
# Motivação

- ▶ Segurança de esquemas de assinatura digital baseada em problemas da teoria de números
  - ▶ Insuficiente no âmbito de algoritmos quânticos
  - ▶ Criptografia pós-quântica é independente destes problemas
- ▶ Funções de mão única são necessárias e suficientes para assinatura digital [Rom90]
  - ▶ Base teórica de funções de resumo criptográfico
  - ▶ Construção de esquemas baseados apenas nestas funções

# Primitivas criptográficas

## Função de resumo criptográfico

$$\mathcal{H} : \{0, 1\}^* \longrightarrow \{0, 1\}^n$$

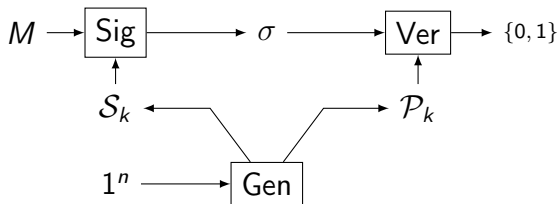


- ▶ SHA-2, SHA-3, BLAKE:  $n \in \{224, 256, 384, 512\}$
- ▶ Keccak: qualquer  $n$
- ▶ Resistência à pré-imagem, segunda pré-imagem, colisões

# Primitivas criptográficas

## Assinatura digital

- ▶ Provê autenticação, integridade e não-repúdio
- ▶ Baseada em criptografia de chaves públicas
- ▶ Tripla de algoritmos probabilísticos de tempo polinomial [Gol04]



- ▶ Existem esquemas onde o par de chaves é de uso único

# Esquema de assinatura única Winternitz

## Etapas de geração de chaves

Tome uma mensagem  $M$ ,  $w \in \mathbb{N}$ ,  $w > 1$ ,  $f : \{0, 1\}^n \rightarrow \{0, 1\}^n$  e  $\mathcal{H} : \{0, 1\}^* \rightarrow \{0, 1\}^n$ . Então,

$$t_1 = \left\lceil \frac{n}{w} \right\rceil, t_2 = \left\lceil \frac{\lfloor \log_2 t_1 \rfloor + 1 + w}{w} \right\rceil \text{ e } t = t_1 + t_2.$$

As chaves privada e pública são, respectivamente,

$$\begin{aligned} \mathcal{S}_k &= (x_{t-1}, \dots, x_0) \xleftarrow{\$} \{0, 1\}^n \text{ e} \\ \mathcal{P}_k &= (f^{2^w-1}(x_{t-1}), \dots, f^{2^w-1}(x_0)) \\ &= (y_{t-1}, \dots, y_0). \end{aligned}$$

# Esquema de assinatura única Winternitz

## Etapas de geração da assinatura

Os valores  $\epsilon_i \in \{0, 1\}^w$  são obtidos como a seguir:

$$\begin{aligned}\mathcal{H}(M) &= \epsilon_{t-1} \parallel \dots \parallel \epsilon_{t-t_1}, & c &= \sum_{i=t-t_1}^{t-1} 2^w - 1 - \epsilon_i, \\ \mathcal{B}_1 &= (\epsilon_{t-1}, \dots, \epsilon_{t-t_1}), & \mathcal{B}_2 &= (\epsilon_{t_2-1}, \dots, \epsilon_0).\end{aligned}$$

Finalmente, a assinatura de uso único é construída:

$$\sigma = (f^{\epsilon_{t-1}}(x_{t-1}), \dots, f^{\epsilon_0}(x_0)).$$

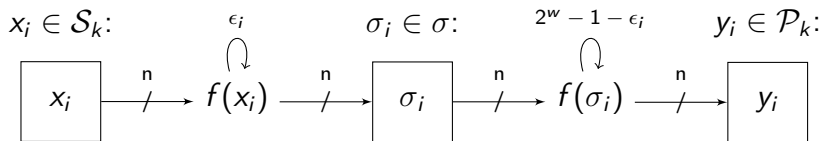
# Esquema de assinatura única Winternitz

## Etapa de verificação da assinatura

Os elementos  $\epsilon_i$  são também utilizados na verificação de  $\sigma$ :

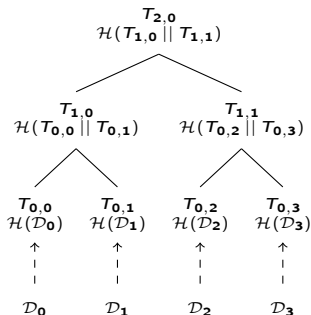
$$\forall \sigma_i \in \sigma, f^{2^w-1-\epsilon_i}(\sigma_i) = y_i.$$

Resumidamente,



# Esquemas baseados em árvores de Merkle

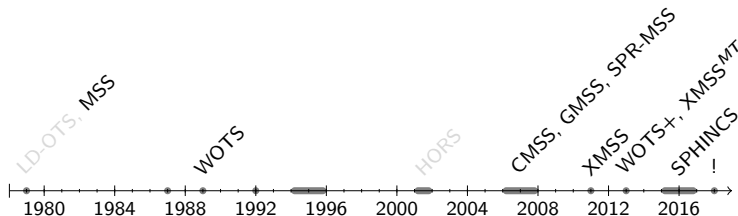
- ▶ Nó construído a partir da concatenação dos resumos de seus filhos
- ▶ Instância de esquema de assinatura única em cada folha da árvore
- ▶ Chaves públicas iniciarão a construção da árvore
- ▶ Winternitz e suas variantes disseminados em esquemas desta família





# Nossas contribuições

## Panorama de esquemas baseados em funções de resumo criptográfico



- Introdução de um parâmetro de compensação no Winternitz
  - Pode ser aplicada em qualquer variante deste esquema
  - Afeta todo esquema baseado em árvores de Merkle

# Nossas contribuições

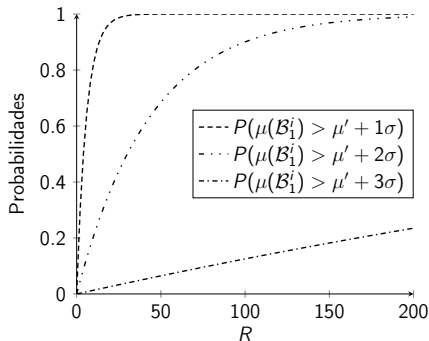
Melhora do desempenho da geração ou verificação de  $\sigma$

- ▶ Modificação de *bits* inutilizados em  $\mathcal{B}_2$ 
  - ▶ Resultados positivos apenas para otimização de Ver
- ▶ Busca de resumos mais eficientes para Sig ou Ver
  - ▶ Modificação da mensagem original através de um *nonce*
  - ▶ Limite de buscas codificado em  $1 \leq i \leq R$
- ▶  $\max(\mu(\mathcal{B}_1^i))$  otimiza Ver, e  $\min(\mu(\mathcal{B}_1^i))$  otimiza Sig
  - ▶ Amplitude de valores para  $\mu(\mathcal{B}_1^i)$  cresce com  $R$

# Nossas contribuições

## Critérios para escolha de $R$

- ▶ Definição de limites para amplitude de  $\mu(\mathcal{B}_1^i)$ 
  - ▶ Assegurar que  $R$  buscas criarão um valor bem-posicionado
  - ▶ Utilização da distribuição binomial
- ▶  $R \in \{25, 200, 3500\}$



# Nossas contribuições

## Resultados

Parâmetros		Winternitz ( $\#f$ )		XMSS (ms)	
$w$	$R$	argmax	argmin	argmax	argmin
4	25	16.71%	16.03%	13.22%	9.48%
	200	22.05%	21.41%	16.08%	-3.60%
	3500	27.64%	27.12%	21.94%	-249.4%
8	25	23.76%	19.32%	22.22%	14.67%
	200	30.96%	26.83%	28.62%	17.23%
	3500	38.45%	34.83%	35.45%	-8.55%
16	25	34.35%	26.53%	—	
	200	43.41%	36.48%		
	3500	52.23%	46.56%		

Aumento de eficiência do esquema com modificações em  $\mu(\mathcal{B}_1^i)$ .

# Referências bibliográficas



O. Goldreich.

*Foundations of Cryptography: Volume 2, Basic Applications.*  
1st edition, 2004.



J. Rompel.

One-way Functions Are Necessary and Sufficient for Secure Signatures.

In H. Ortiz, editor, *Proceedings of the Twenty-second Annual ACM Symposium on Theory of Computing*, pages 387–394, May 1990.