

Esquemas de assinatura digital baseados em funções de resumo

Aprimoramento de esquemas antigos

Gustavo Zambonin

Universidade Federal de Santa Catarina
Departamento de Informática e Estatística

Esquemas introdutórios

- ▶ Lamport-Diffie tem assinaturas e pares de chaves muito grandes
- ▶ Merkle (MSS) verifica um número limitado de assinaturas com sua chave pública, e não é eficiente de modo geral
- ▶ novos esquemas, mais eficientes e seguros

Esquema de assinatura de Winternitz [1, 2]

- ▶ aplica-se a função \mathcal{H} repetidamente em uma entrada secreta
- ▶ número de iterações depende da mensagem a ser assinada
- ▶ parâmetro $w \in \mathbb{N}$ define o número de bits a serem assinados simultaneamente
- ▶ notação
 - ▶ $\xleftarrow{\$}$: "gerado aleatoriamente de"
 - ▶ $\Delta^{(x_1, x_2)}$: x_2 palavras de tamanho x_1 compostas pelo alfabeto Δ
 - ▶ $\mathcal{H}^x(m) = \mathcal{H}(\mathcal{H}^{x-1}(m))$, $\mathcal{H}^0(m) = m$


Winternitz – descrição do algoritmo

- ▶ \mathcal{G} : $t_1 = \lceil \frac{n}{w} \rceil$, $t_2 = \lceil \frac{\lfloor \log_2 t_1 \rfloor + 1 + w}{w} \rceil$, $t = t_1 + t_2$
 $S_k = (y_{t-1}, \dots, y_0) \xleftarrow{\$} \{0, 1\}^{(n, t)}$
 $P_k = (\mathcal{H}^{2^w-1}(y_{t-1}), \dots, \mathcal{H}^{2^w-1}(y_0))$
- ▶ \mathcal{S} : $\mathcal{H}(m) + \text{padding} = (p_{t-1}, \dots, p_{t-t_1}) \in \{0, 1\}^{(w, t_1)}$
 $c = \sum_{i=t-t_1}^{t-1} (2^w - p_i)$
 $c \leq t_1 2^w$, $c + \text{padding} = (p_{t_2-1}, \dots, p_0)$
 $\mathcal{S}(\mathcal{H}(m)) = (\mathcal{H}^{p_{t-1}}(y_{t-1}), \dots, \mathcal{H}^{p_0}(y_0))$
- ▶ \mathcal{V} : $\forall \sigma_i \in \mathcal{S}(\mathcal{H}(m))$, $\mathcal{H}^{2^w-1-p_i}(\sigma_i) = P_{k_i}$, $0 \leq i \leq t-1$

 D. J. Bernstein, J. Buchmann, and E. Dahmen.

Post Quantum Cryptography.

Springer Publishing Company, Incorporated, 1st edition, 2008.

 J. Buchmann, E. Dahmen, S. Erath, A. Hülsing, and M. Rückert.

On the Security of the Winternitz One-time Signature Scheme.

In *Proceedings of the 4th International Conference on Progress in Cryptology in Africa*, AFRICACRYPT'11, pages 363–378, Berlin, Heidelberg, 2011. Springer-Verlag.