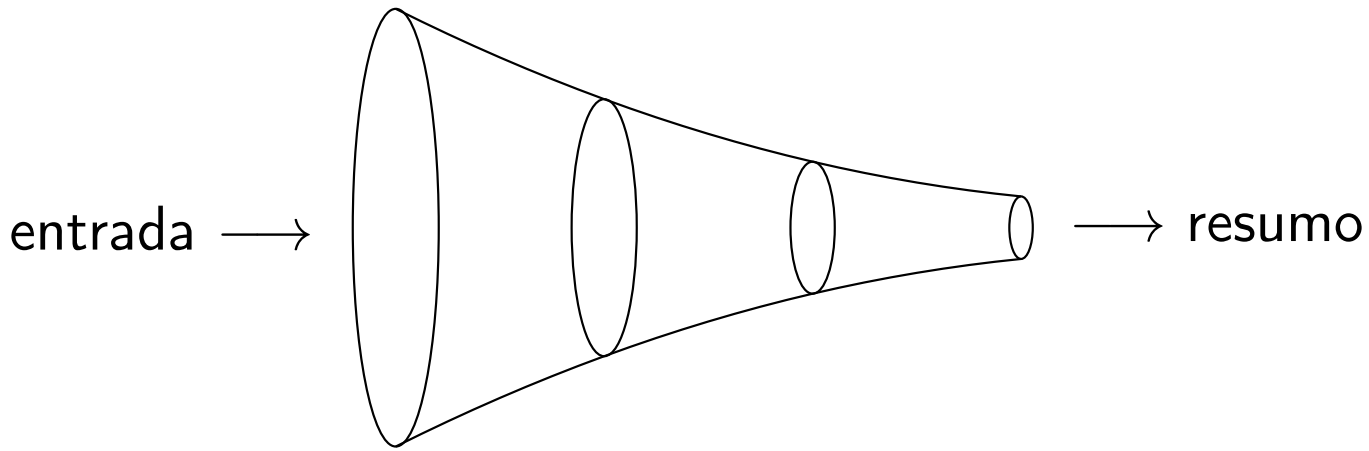
Esquemas de assinatura digital baseados em funções de resumo

Gustavo Zambonin

Universidade Federal de Santa Catarina
Departamento de Informática e Estatística
INE5453 - Introdução ao Trabalho de Conclusão de Curso

Funções de resumo criptográfico

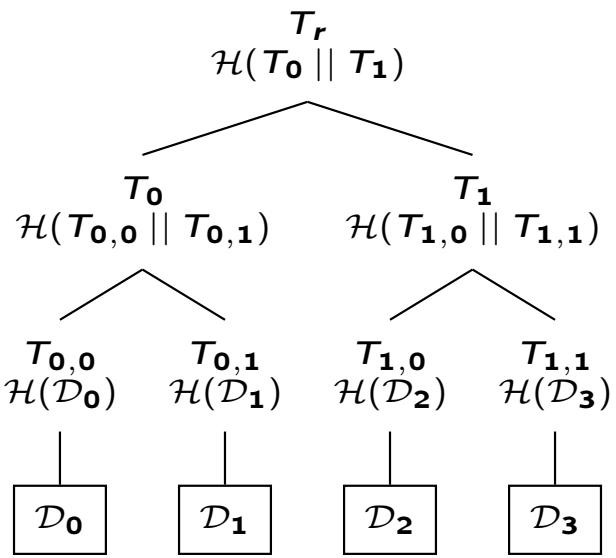
$$\mathcal{H} : \{0,1\}^* \longrightarrow \{0,1\}^n$$



- RIPEMD: $n \in \{128, 160, 256, 320\}$
- SHA-2, SHA-3, BLAKE: $n \in \{224, 256, 384, 512\}$
- Keccak: n arbitrário

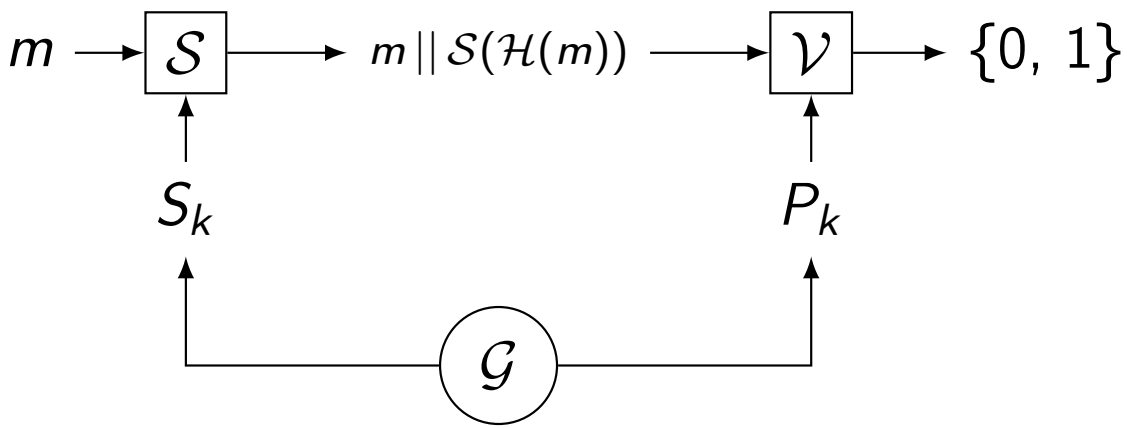
Árvore de Merkle [7]

- $\mathcal{H}(m)$ é uma função de resumo aplicada sobre uma mensagem m
- $||$ é o operador de concatenação de palavras
- $\mathcal{D}_n$ é um bloco de dados qualquer



Assinatura digital

- busca prover autenticação, integridade e não-repúdio
- baseada em criptografia assimétrica
  - chaves pública (P_k) e privada (S_k) para uma entidade
- consiste de uma tripla de algoritmos [5]
  - geração de chaves ($\mathcal{G}$), assinatura de mensagens ($\mathcal{S}$), verificação da assinatura ($\mathcal{V}$)
- deve existir uma maneira de ligar o assinante à chave



Esquema de assinatura de Lamport–Diffie [6]

- acredita-se ser seguro o suficiente em computadores quânticos
- par de chaves deve ser utilizado uma única vez
  - cada uso posterior divide o nível de segurança pela metade
- descrição do algoritmo
  - $\mathcal{G}$: $S_k = \{y_{i,j} : 1 \leq i \leq n,\ j \in \{0,1\}\}$ gerados aleatoriamente
    $P_k = \{\mathcal{H}(y) : y \in S_k\}$
  - $\mathcal{S}$: $\mathcal{H}(m) = h_1, \ldots h_n \in \{0,1\}$
    $\mathcal{S}(\mathcal{H}(m)) = (y_{1,h_1}, \ldots, y_{n,h_n})$
  - $\mathcal{V}$: $\forall y_{i,h_i} \in \mathcal{S}(\mathcal{H}(m)),\ \mathcal{H}(y_{i,h_i}) = P_{k_{i,h_i}}, 1 \leq i \leq n$

Esquema de assinatura de Merkle

- árvore de Merkle + esquema de assinatura única (e.g. Lamport)
- assina um número limitado ($t \leq 25$) de mensagens $\{m_1, \ldots, m_{2^t}\}$
- definição do algoritmo para uma árvore T
  - $\mathcal{G}$: $\mathbf{S_k} = \{(S_{k_i}, P_{k_i}) : 1 \leq i \leq 2^t\}$
    $\mathbf{P_k} = \mathcal{H}(T_r)$, com $\{\mathcal{H}(P_{k_i}) : 1 \leq i \leq 2^t\}$ como folhas da árvore
  - $\mathcal{S}$: escolha de um par não utilizado (S_{k_i}, P_{k_i}), produz $\mathcal{S}'$
    $A = a_0, \ldots, a_n$ (irmãos dos nodos do caminho até à raiz)
    $\mathcal{S}(m_i) = \{\mathcal{S}' \,||\, P_{k_i} \,||\, a_0 \,||\, \ldots \,||\, a_n\}$
  - $\mathcal{V}$: verifica $\mathcal{S}'$ e constrói a sub-árvore T'; $\mathcal{H}(T'_r) = \mathbf{P_k}$

Esquemas mais complexos

- Winternitz (1989, [4])
  - baseado em aplicações repetidas de $\mathcal{H}$
  - assinaturas muito menores
  - processo de verificação mais eficiente
- CMSS (2005, [1])
  - encadeamento de árvores
  - 2^{40} mensagens
  - guarda apenas a semente do PRNG em P_k
- GMSS (2007, [3])
  - *Generalized Merkle Signature Scheme*
  - 2^{80} mensagens
- XMSS (2011, [2])
  - *eXtended Merkle Signature Scheme*
  - uma mensagem comprometida não expõe outras (*forward secrecy*)

Referências I


J. Buchmann, L. C. Coronado García, E. Dahmen, M. Döring, and E. Klintsevich.
CMSS – An Improved Merkle Signature Scheme.
In R. Barua and T. Lange, editors, *Progress in Cryptology - INDOCRYPT 2006*, pages 349–363, Kolkata, India, 2006. Springer-Verlag Berlin Heidelberg.


J. Buchmann, E. Dahmen, and A. Hülsing.
XMSS – A practical forward secure signature scheme based on minimal security assumptions.
In B. Yang, editor, *PQCrypto 2011*, pages 117–129, Taipei, Taiwan, 2011. Springer-Verlag Berlin Heidelberg.


J. Buchmann, E. Dahmen, E. Klintsevich, K. Okeya, and C. Vuillaume.
Merkle Signatures with Virtually Unlimited Signature Capacity.
Lecture Notes in Computer Science, 4521:31–45, 2007.

Referências II


C. Dods, N. Smart, and M. Stam.
Hash Based Digital Signature Schemes.
Lecture Notes in Computer Science, 3796:96–115, 2005.


O. Goldreich.
Foundations of Cryptography: Volume 2, Basic Applications.
Cambridge University Press, New York, NY, USA, 2004.


L. Lamport.
Constructing Digital Signatures from a One Way Function.
SRI International, 1979.


R. C. Merkle.
Method of providing digital signatures, 1982.
US Patent 4,309,569.