Esquemas de assinatura digital pós-quânticos baseados em AES

Gustavo Zambonin Marcello Klingelfus

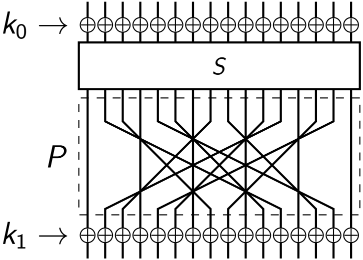
Universidade Federal de Santa Catarina
Departamento de Informática e Estatística
INE5424 — Sistemas Operacionais II

{gustavo.zambonin,marcello.klingelfus}@grad.ufsc.br

Motivação

- Segurança de esquemas de assinatura digital é baseada em teoria de números ou problemas algébricos
  - Insuficiente no âmbito de computadores 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
  - Livre escolha, critério situacional (hardware, software)
  - Cifras de bloco são utilizadas em sua construção [MVO96, Sec. 9.14]

- Versão padronizada pelo NIST do algoritmo Rjindael [DR02]
  - Principais escolhas de design: inversibilidade e eficiência
- Cifra de blocos parametrizada por uma chave K
- Conceito de rede de substituição-permutação



Exemplo de rede de substituição-permutação com apenas uma rodada. Note que P pode ser substituída por vários passos de difusão.

- $|K| \in \{128, 192, 256\}$
  - 10, 12 ou 14 rodadas (n_r), respectivamente
- P é composta de dois passos
- Modifica uma matriz de estado A, $A_{i,j} \in \mathbb{F}_{2^8}, 0 \leq i, j \leq 3$
  - Para uma mensagem m, $A_{i,j} = m_{i+4j}$
- Operações sobre bytes análogas a cálculos em $\mathbb{F}_{2^8}$
  - Adição equivalente a "ou exclusivo"
  - Multiplicação usual, módulo o polinômio irredutível $x^8 + x^4 + x^3 + x + 1$

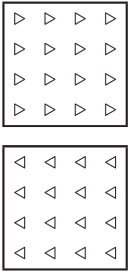
AES

Etapa *SubBytes*

- Caixa de substituição (*S-box*) aplicada em cada $A_{i,j}$ individualmente
- Única etapa não-linear da cifra
- Transformação afim sobre $a = A_{i,j}^{-1}$

$$A'_{i,j} = \begin{matrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{matrix} \cdot \begin{matrix} a_0 \\ a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \\ a_6 \\ a_7 \end{matrix} + \begin{matrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{matrix}$$

- *InvSubBytes*: inversa da transformação afim



Pictogramas para as etapas *SubBytes* (acima) e sua inversa *InvSubBytes*.

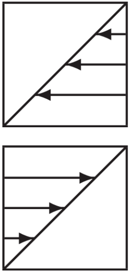
AES

Etapa *ShiftRows*

- Rotacionamento cíclico das linhas de A
- Provê difusão, impede que a cifra aja separadamente sobre as linhas

$$\begin{matrix} a & b & c & d \\ e & f & g & h \\ i & j & k & l \\ m & n & o & p \end{matrix} \longrightarrow \begin{matrix} a & b & c & d \\ f & g & h & e \\ k & l & i & j \\ p & m & n & o \end{matrix}$$

- *InvShiftRows*: rotacionamento inverso

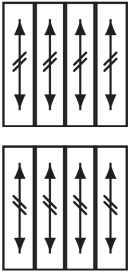


Pictogramas para as etapas *ShiftRows* (acima) e sua inversa *InvShiftRows*.

- Permutação operando em cada coluna de A, também provendo difusão
- $a = A_j$ tratada como um polinômio e multiplicada por uma constante

$$a' = (a_3x^3 + a_2x^2 + a_1x^1 + a_0x^0) \\ \cdot (3x^3 + x^2 + x + 2) \pmod{x^4 + 1}$$

- *InvMixColumns*: multiplicação por $(3x^3 + x^2 + x + 2)^{-1}$



Pictogramas para as etapas *MixColumns* (acima) e sua inversa *InvMixColumns*.

- *KeyExpansion*: chave expandida K^e, $\ell = \frac{|K|}{32}$ palavras por rodada
- "*Round constants*":
  $RC_0 = x^0, RC_1 = x^1, RC_j = x^{j-1} \cdot RC_{j-1}, j > 2$

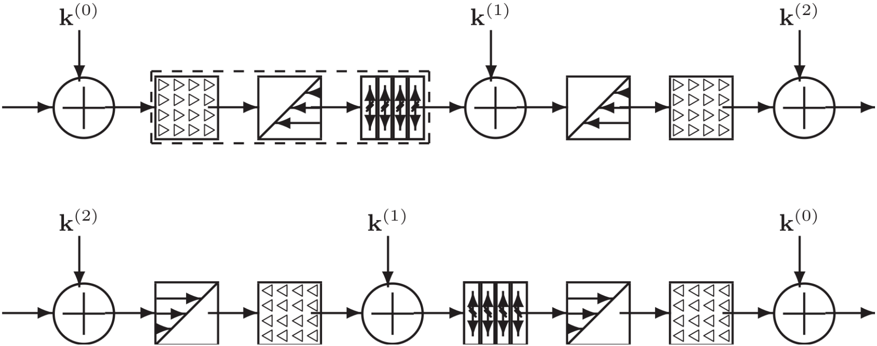
$$K^e = (\overbrace{k_0, \ldots, k_{\ell-1}}^{K}, k_\ell, \ldots, k_{(n_r+1)\cdot\ell-1})$$

$$k_i = k_{i-\ell} + \begin{cases} \text{SubBytes}(k_{i-1} \overset{\curvearrowright}{\ll} 8) + RC_{\frac{i}{\ell}}, & \text{se } i \equiv 0 \pmod 4 \\ \text{SubBytes}(k_{i-1}), & \text{se } \ell = 8 \text{ e } i \equiv 4 \pmod 8 \\ k_{i-1}, & \text{caso contrário.} \end{cases}$$

- *AddRoundKey*: $A' = A + (k_{\ell\cdot i}, \ldots, k_{\ell\cdot(i+1)-1}), 0 \leq i \leq n_r$

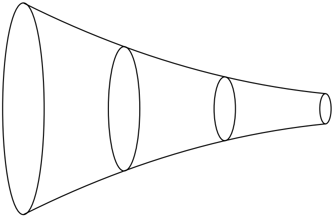
AES

Representação gráfica da codificação e decodificação para $n_r = 2$



Funções de resumo criptográfico

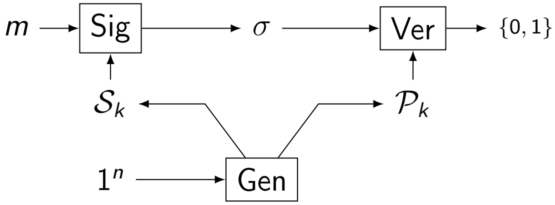
$$\mathcal{H} : \{0,1\}^* \longrightarrow \{0,1\}^n$$

entrada $\longrightarrow$  $\longrightarrow$ resumo

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

Assinatura digital

- Provê autenticação, integridade e não-repúdio
- Baseado em criptografia de chaves públicas
- Tripla de algoritmos probabilísticos de tempo polinomial [Gol04]
  - Geração de chaves (*Gen*), geração da assinatura (*Sig*), verificação da assinatura (*Ver*)



Esquemas de assinatura única

- Par de chaves só deve ser utilizado uma única vez
- Lamport-Diffie (LD-OTS)
  - Primeiro esquema baseado em resumos
  - Mensagens de tamanho arbitrário podem ser assinadas, um bit por vez
- Winternitz (WOTS)
  - Múltiplos bits podem ser assinados simultaneamente
  - Generalização do LD-OTS
  - Compensação entre desempenho e tamanho da assinatura

Seja $w \in \mathbb{N}, w > 1$ o parâmetro Winternitz, $f : \{0,1\}^n \longrightarrow \{0,1\}^n$ e $\mathcal{H} : \{0,1\}^* \longrightarrow \{0,1\}^n$. 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,

$$\mathcal{S}_k = (y_{t-1}, \ldots, y_0) \xleftarrow{\$} \{0,1\}^n \text{ e}$$
$$\mathcal{P}_k = (f^{2^w - 1}(y_{t-1}), \ldots, f^{2^w - 1}(y_0)).$$

Os valores $\epsilon_i \in \{0,1\}^w$ são obtidos através de:

$$\mathcal{H}(m) = (\epsilon_{t-1}, \ldots, \epsilon_{t-t_1})$$

$$\begin{aligned} c &= \sum_{i=t-t_1}^{t-1} (2^w - 1 - \epsilon_i) \\ &= (\epsilon_{t_2-1}, \ldots, \epsilon_0) \end{aligned}$$

Finalmente, a assinatura de uso único é construída:

$$\sigma = (f^{\epsilon_{t-1}}(y_{t-1}), \ldots, f^{\epsilon_0}(y_0))$$

Winternitz OTS

Verificação

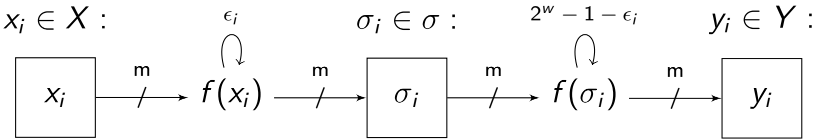
Relembrando,

$$\mathcal{P}_k = (f^{2^w-1}(y_{t-1}), \dots, f^{2^w-1}(y_0)) \text{ e}$$
$$\sigma = (f^{\epsilon_{t-1}}(y_{t-1}), \dots, f^{\epsilon_0}(y_0)).$$

Os elementos ϵ_i são calculados e utilizados na verificação de σ:

$$\forall \sigma_i \in \sigma, f^{2^w-1-\epsilon_i}(\sigma_i) = \mathcal{P}_{k_i}$$

Resumidamente,

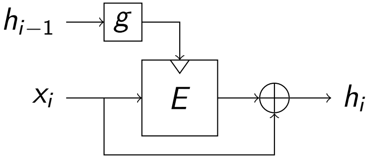


- Elimina a necessidade de $\mathcal{H}$ resistente a colisões
  - Modificação da função de iteração f para uma família $\mathcal{F}_k : \{f_k : \{0,1\}^n \longrightarrow \{0,1\}^n \mid k \in \mathcal{K}_n\}$
- Máscaras de bits aleatórias em cada iteração

$$
\begin{aligned}
r = (r_0, \ldots, r_{2^w-1}) &\xleftarrow{\$} \{0,1\}^n \\
c_k^0(x, r) &= x \\
c_k^i(x, r) &= f_k(c_k^{i-1}(x, r) \oplus r_i).
\end{aligned}
$$

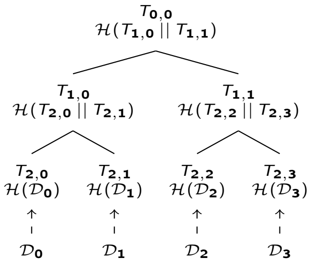
- Derivação de f a partir de uma cifra de bloco

- Construção Matyas-Meyer-Oseas [MVO96, Sec. 9.41]
  - Tome uma cifra E_K com bloco de n bits
  - Divida a entrada em k blocos de n bits, $X = (x_0, \ldots, x_{k-1})$
  - Tome um valor inicial IV e uma função g que gere chaves válidas para E
  - $h_0 = IV, h_i = E_{g(h_{i-1})}(x_i) \oplus x_i, 1 \leq i \leq k$



Esquemas baseados em árvores de Merkle

- Assinaturas únicas em cada folha, árvore construída a partir de chaves públicas
- Estado da arte dos esquemas baseados em funções de resumo criptográfico
- XMSS, XMSS^{MT}, SPHINCS



Seja $\mathcal{D}_n$ um dado qualquer. Uma árvore de Merkle é construída recursivamente através da concatenação dos resumos dos filhos de um nó.

Bibliografia I

Joan Daemen and Vincent Rijmen.
The Design of Rijndael.
Springer-Verlag New York, Inc., Secaucus, NJ, USA, 2002.

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

Alfred J. Menezes, Scott A. Vanstone, and Paul C. Van Oorschot.
Handbook of Applied Cryptography.
CRC Press, Inc., Boca Raton, FL, USA, 1st edition, 1996.

Bibliografia II

J. Rompel.
One-way Functions Are Necessary and Sufficient for Secure Signatures.
In *Proceedings of the Twenty-second Annual ACM Symposium on Theory of Computing*, STOC '90, pages 387–394, New York, NY, USA, 1990. ACM.