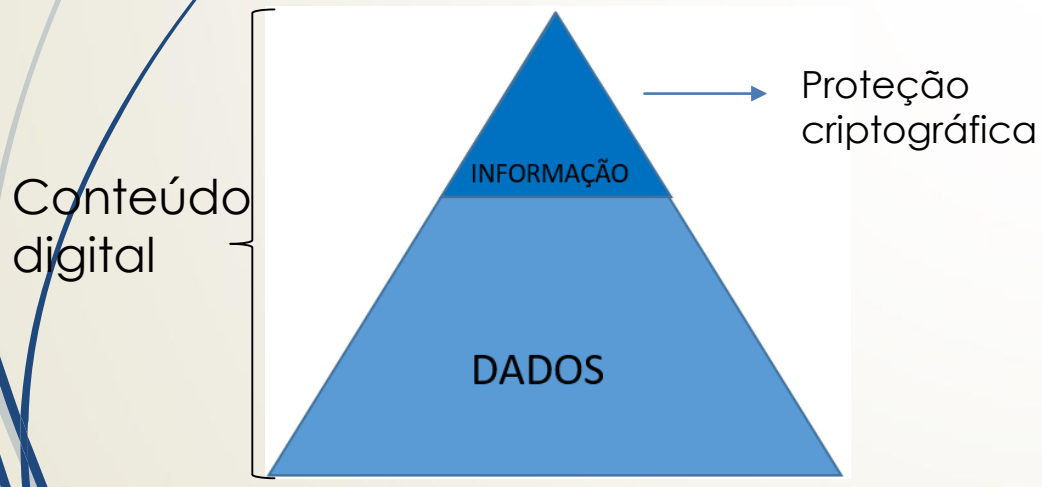
Implementação do Algoritmo Criptográfico Leve Simon

Cláudio Roberto Costa

Contextualização

- Segurança de informação (criptografia)
- Conteúdo digital (Informação x Dados)
- Cifras de bloco leve (Simon)



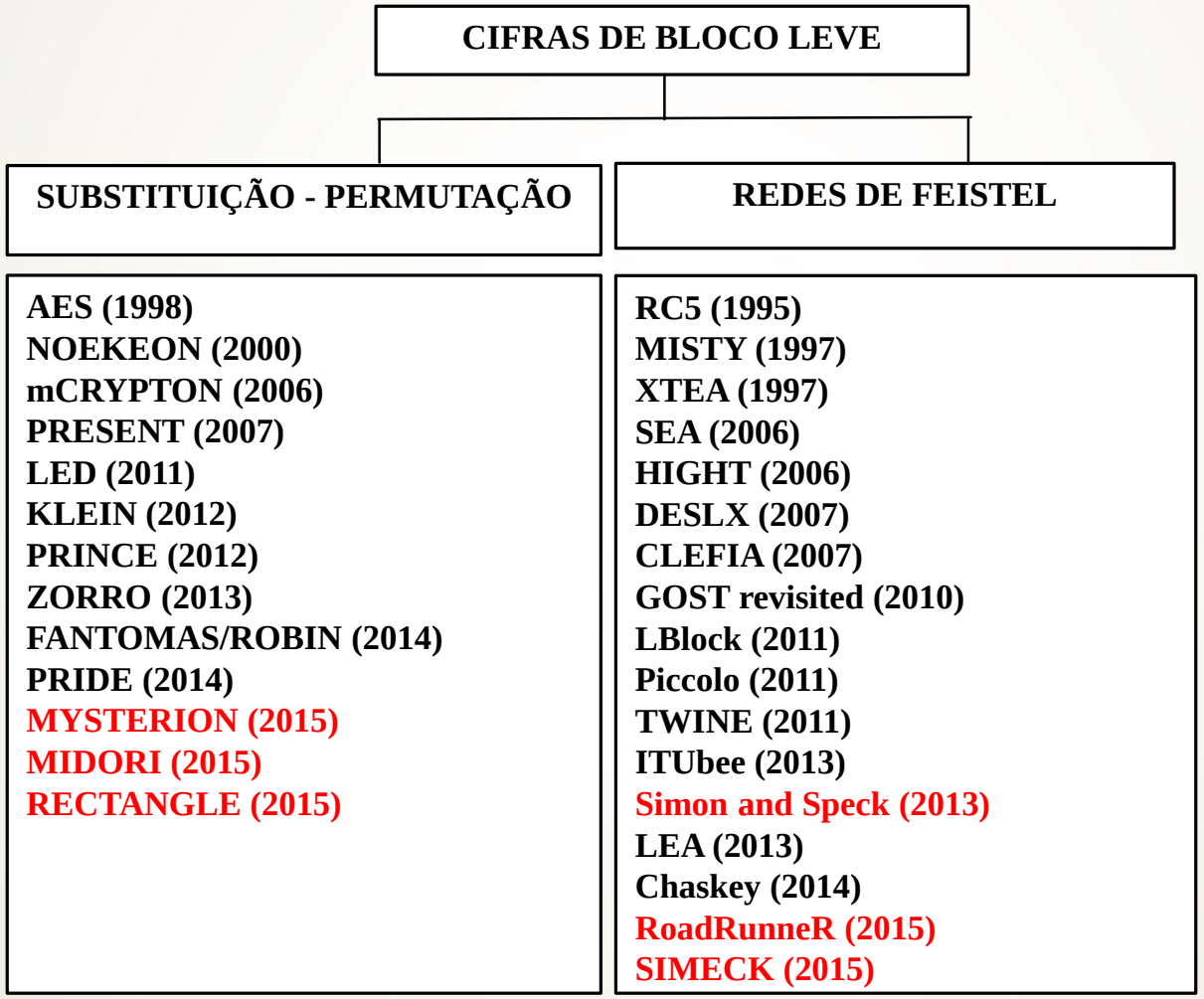
Fonte: Elaborada pelo autor

Aplicações

- *Internet of Things* – IoT (Internet das Coisas)
- Computação Pervasiva ou Ubíqua
- Sistemas Embarcados

CIFRAS DE BLOCO LEVE

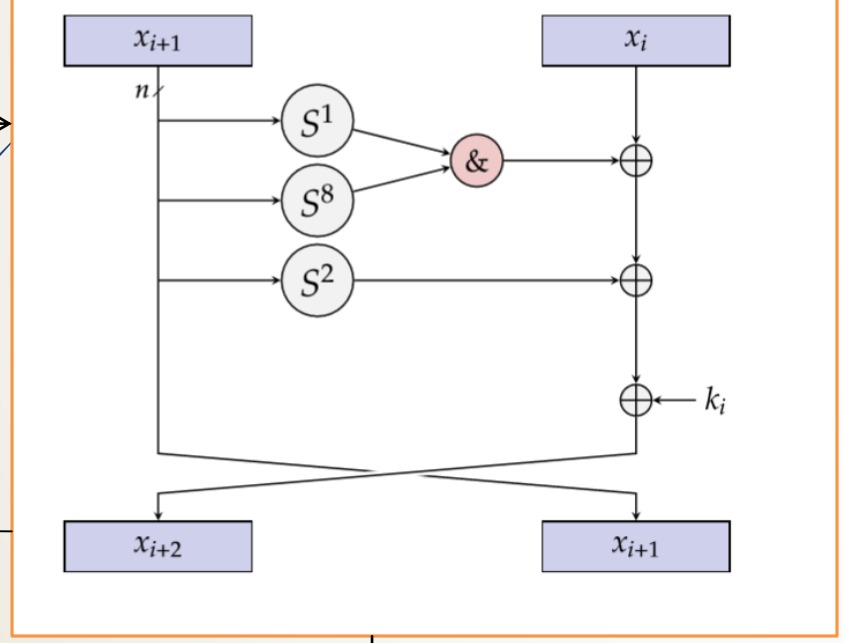
- Classificação por estrutura



Fonte: Elaborada pelo autor

Algoritmo Simon

Bloco Texto (M)



Bloco Cifrado (C)

Chave (K)

Produz sub-chaves a partir da chave K

Cada sub-chave é utilizada em uma rodada (n) do SIMON

n

- XOR bit a bit - $\oplus$
- AND bit a bit - &
- Deslocamento circular - S^n

Pseudocódigo Simon 32

PARA i = 0 .. T-1

$tmp = x$

$x = y \oplus (Sx \,\&\, S^8x) \oplus S^2x \oplus k_i$

$y = tmp$

FIM PARA

T = 32

k_i = chave da rodada

Expansão das Chaves

PARA i = m .. T-1

$tmp = S^{-3} k_{i-1}$

Se (m=4)

$tmp = \text{tmp} \oplus k_{i-3}$

$tmp = \text{tmp} \oplus S^{-1} tmp$

$k_i = not\ k_{i-m} \oplus tmp \oplus z[j][(i-m) mod 62] \oplus 3$

FIM PARA

T = 32

k_i = chave da rodada

Z = constante

m = 4

Objetivo

O objetivo deste trabalho a implementação do algoritmo de cifras de bloco leve Simon utilizando paralelismo.

Referências

- Beaulieu, R., Shors, D., Smith, J., Treatman-Clark, S., Weeks, B., and Wingers, L. The Simon and Speck Families of Lightweight Block Ciphers. Cryptology ePrint Archive, Report 2013/404 (2013). https://eprint.iacr.org.
- ISO/IEC 27001, Information Security Management System (ISMS), 2005
- Vortice 2015, O que é BI?. http://www.vortice.inf.br/noticia/http-blog-prgbrasil-com-2015-06-19-o-que-e-bi-preview-id222

Implementação do Algoritmo Criptográfico Leve Simon