SystemC IDEA

Lucas Avelino - 13/0013072
Lucas Nascimento - 14/0151010

1.

IDEA

IDEA (International Data Encryption Algorithm) é um algoritmo com *chave secreta* de 128 bits e tanto o *texto legível* (entrada) quanto o *texto ilegível* (saída) de 64 bits.

- Possui um número fixo de *rounds* de uma mesma função que utiliza *sub-chaves* distintas;
- O mesmo algoritmo serve para *criptografar* e *decriptografar*, alterando apenas a forma de geração das sub-chaves.

- É conhecido publicamente desde 1991 e até agora não foram reveladas vulnerabilidades, mesmo aposś anos de criptoanálise feita por especialistas.

2.

Estrutura do IDEA

XOR

Ou-exclusivo de dois operandos de 16 bits (Detonado pelo símbolo $\oplus$).

ADIÇÃO mod 2^{16}

Adição de dois operandos de 16 bits, ignorando qualquer *overflow* (Denotado pelo símbolo $\boxplus$).

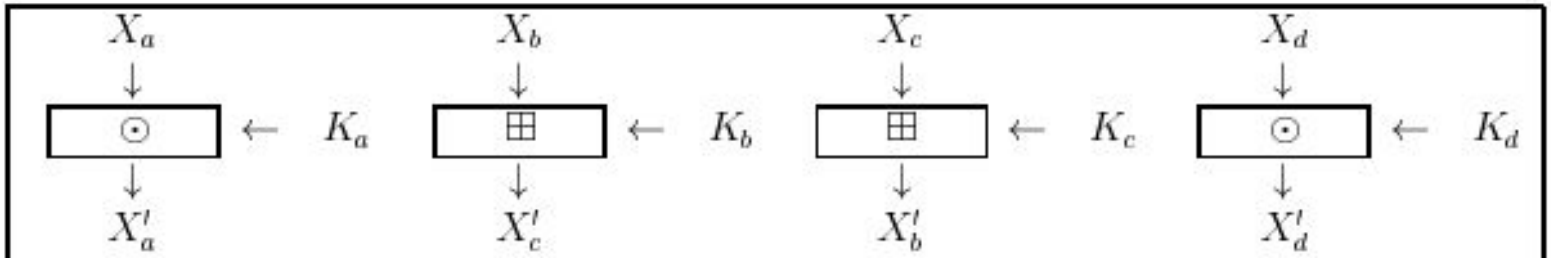
MULTIPLICAÇÃO mod $2^{16}+1$

Multiplicação de dois operandos de 16 bits, ignorando qualquer *overflow* (Denotado pelo símbolo $\odot$).

- A partir da chave secreta de 128 bits, são geradas 52 *sub-chaves* (K_1, K_2, K_3, ...,K_{52}) de 16 bits.

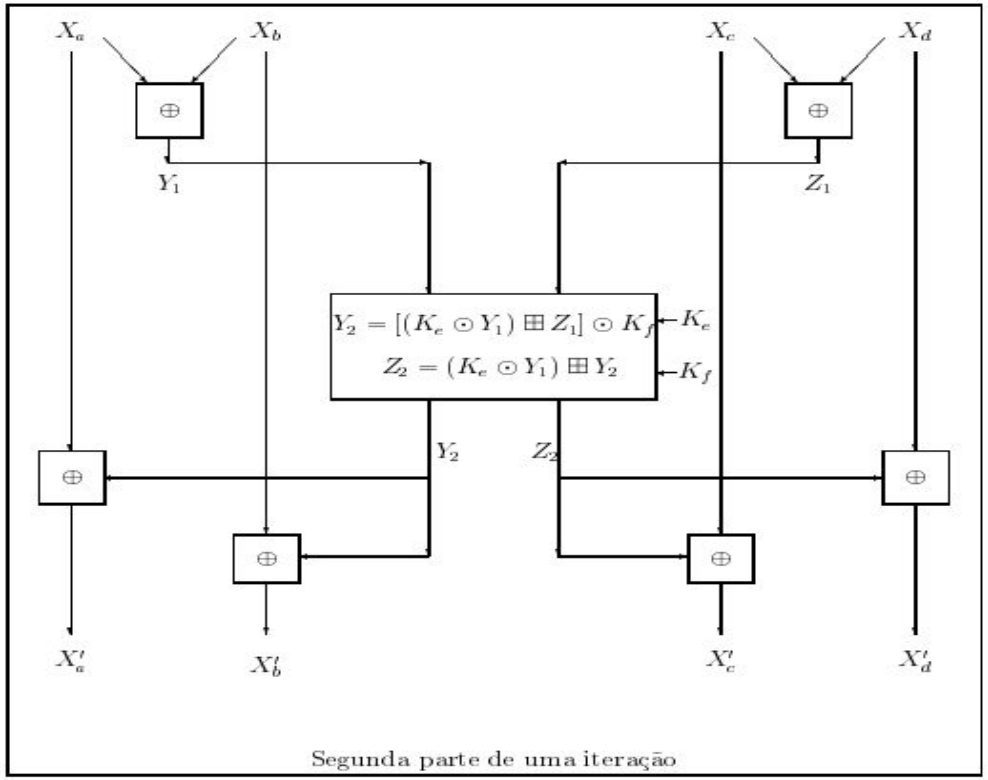
(nº de *rounds*)x(nº de *sub-chaves* de um round)+
(nº de *sub-chaves* do *half-round*) =
(8x6)+4 = 52

- Cada iteração é subdividida em duas partes:
  1. A *primeira* utiliza 4 *sub-chaves* K_a, K_b, K_c, K_d e uma entrada de 64 bits tratada como 4 *sub-entradas* de 16 bits X_a, X_b, X_c, X_d para obter as saídas X_a', X_b', X_c', X_d'.

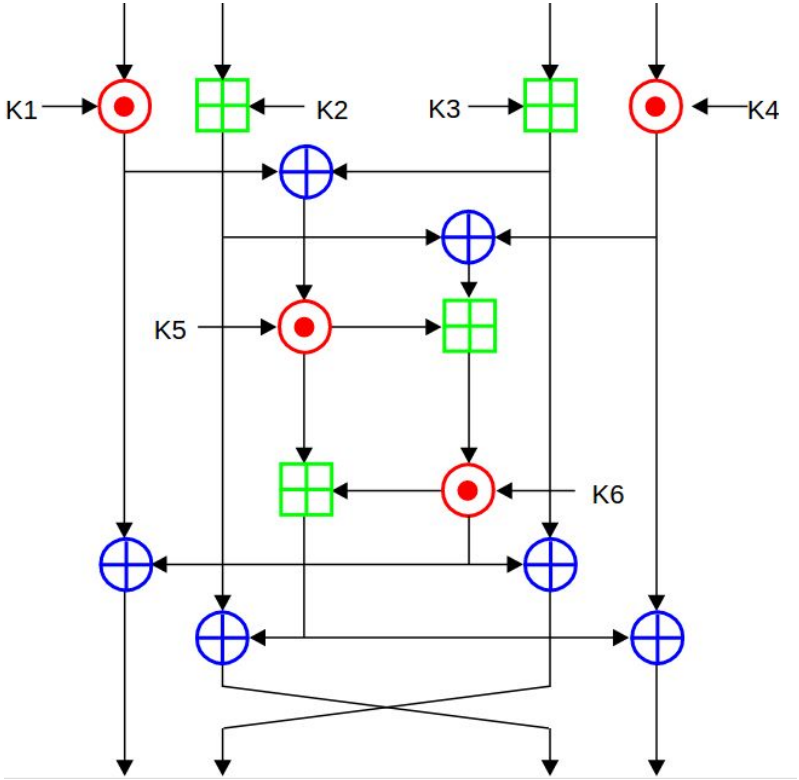


Primeira parte de uma iteração

2 A *segunda* utiliza duas *sub-chaves* K_e e K_f que são operadas com as 4 saídas de 16 bits da primeira parte X_a, X_b, X_c, X_d para formar novos X_a', X_b', X_c', X_d'.

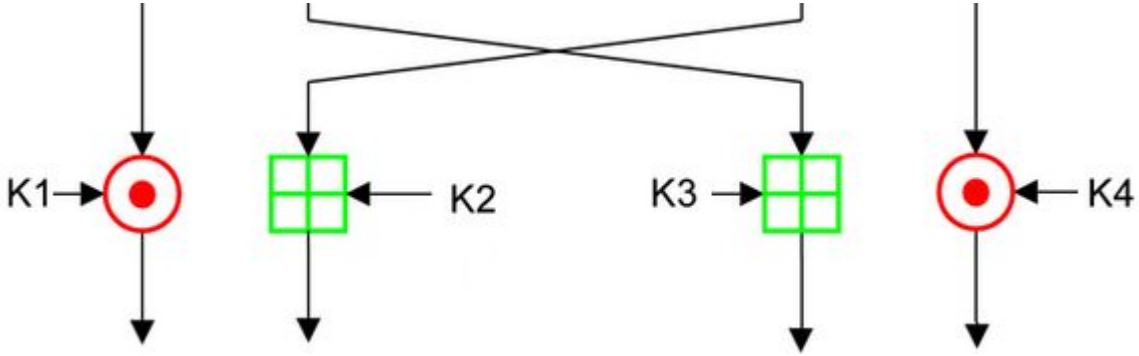


Segunda parte de uma iteração

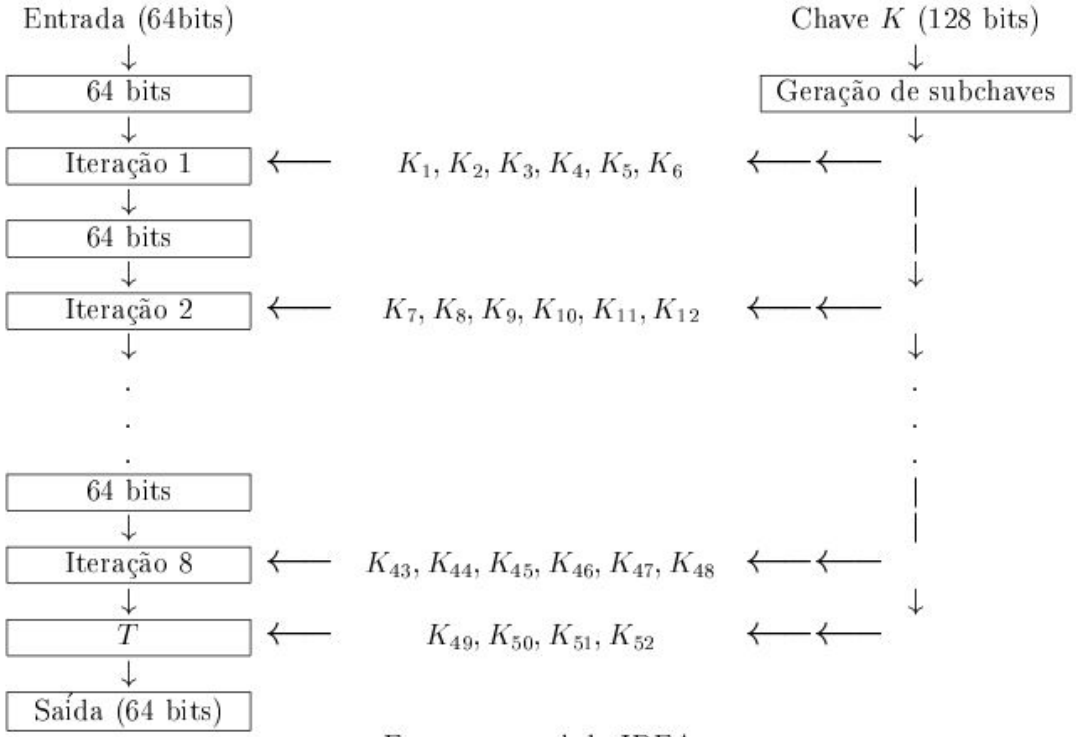


Representação de um *round*, que é a junção da primeira e segunda parte de uma iteração.

- Após 8 repetições de um *round*, o resultado X_a', X_b', X_c', X_d' é fornecido como entrada para a última transformação T, também conhecida como *half-round*.
- As operações realizadas são idênticas às da primeira parte de cada iteração, com uma pequena diferença na ordem das chaves para as operações.



Half-round, o último passo do processo de criptografia.



Esquema geral do IDEA

- O IDEA foi feito de forma que o mesmo circuito ou software serve para criptografar ou decriptografar 64 bits.
- As 3 operações básicas do IDEA são facilmente inversíveis, e portanto não é complicado de se obter as subchaves inversas.
- Para realizar a decriptação é necessário:

- Calcular previamente as *sub-chaves* inversas para a primeira parte do algorítmo.
- A segunda parte é exatamente a mesma para encriptação e decriptação e portanto pode ser executada normalmente.
- Inverter a ordem em que as chaves são utilizadas

3.

Implementação em SystemC

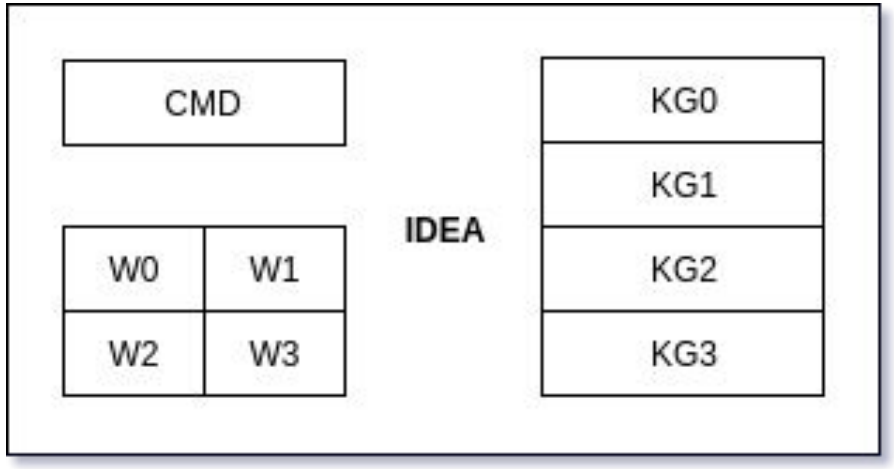


Diagrama que representa a implementação do IDEA em SystemC.

- Os registradores (32 bits) são:
  - **[W0, W1], [W2, W3]**: Entrada de 64 bits dividida em 4 palavras;
  - **[KG0], [KG1], [KG2], [KG3]**: Chave secreta, utilizada para gerar as *sub-chaves* das iterações;
  - **[CMD]**: Comandos de controle.

- Gerar chaves para descifrar
- Gerar chaves para cifrar
- Descifrar
- Cifrar
- Status

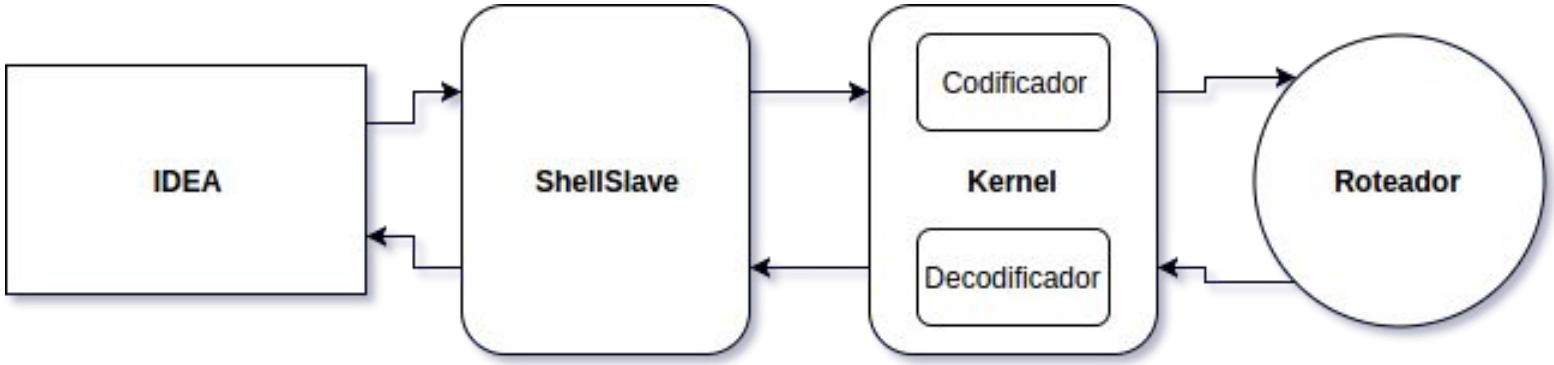


Diagrama que representa a conexão do módulo IDEA com a NoC.

Modelagem de Sistemas em Silício 1/2017
Professor Ricardo Jacobi

Grupo IDEA
Lucas Avelino - 13/0013072
Lucas Nascimento - 14/0151010