MODULAR EXPONENTIATION

Computação Reconfigurável
2024/2025

RUI LAMEIRAS 102817 LEANDRO RITO 92975

deti universidade de aveiro
departamento de eletrónica, telecomunicações e informática

universidade de aveiro

OBJETIVO PARA COM O TRABALHO

RSA é um cifra muito importante para a criptografia e, devido a isso, é muito usada em por exemplo mensagens, etc levando a uma necessidade de sua otimização para evitar longas gerações de chave e encriptação e decriptação de mensagens
Como tal, o nosso trabalho visa acelerar a cifra e decifra de em RSA

PARA EFETUARMOS USAMOS AXI4-LITE

- Possibilidade de simular comunicação normal do género TCP
- Permite um melhore controlo sobre a operação do modulo de exponiciação

O MODULO DE EXPONENCIAÇÃO

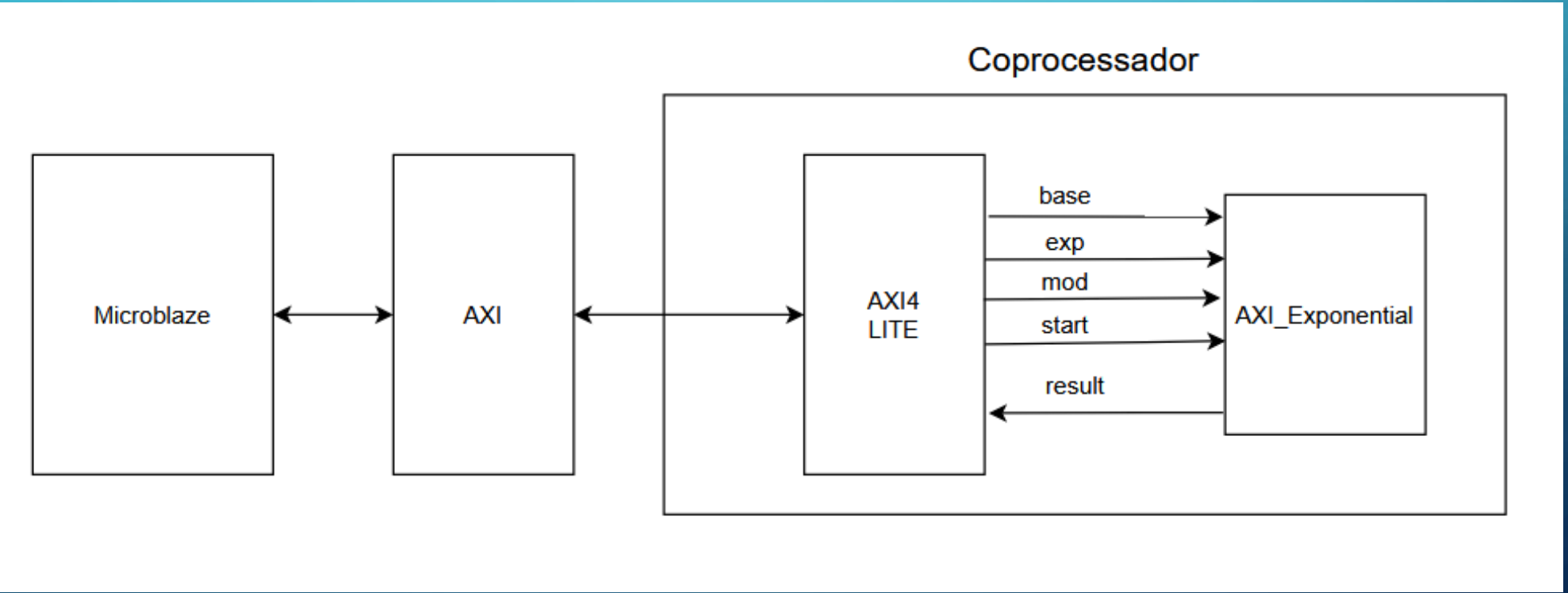
$$c = b^e \bmod m$$

c - cifra
b - base
e - expoente
m - modulo

ALGORITMO COMPLETO

1. Geração de 2 números primos p e q
2. Geração da chave pública () e chave privada utilizando os números primos
3. Encriptação da mensagem utilizando a chave pública, gerando uma cifra
4. Decriptação da cifra utilizando a chave privada, gerando a mensagem

DIAGRAMA


Coprocessador
Microblaze
AXI
AXI4
LITE
base
exp
mod
start
result
AXI_Exponential

DEMO

PROBLEMAS

- Encriptação com defeito
- Tempo de síntese e implementação elevado, dificultando testes do coprocessador

DUVIDAS

FIM