

Proyecto I

Diseño e Implementación de un ASIP de descryptación mediante RSA

Alejandro Soto Chacón, 2019008164
CE4301: Arquitectura de Computadores I
Instituto Tecnológico de Costa Rica

I. DISEÑO

I-A. Requerimientos

I-B. Opciones para ISA base

I-B1. x86-64:

I-B2. AArch64:

I-B3. RV64I:

I-C. Exponenciación modular

I-D. Técnicas de división de enteros

I-D1. División por hardware:

I-D2. Inverso multiplicativo modular:

I-D3. Aritmética de punto fijo:

I-E. Oportunidades de optimización en el caso concreto

I-E1. Respecto a límites conocidos:

I-E2. Memoización de la relación ciphertext-plaintext:

I-E3. Vectorización del bucle principal:

I-F. Propuestas de solución

I-F1. RV64IMV:

I-F2. x86-64, AVX2:

I-G. Comparación de propuestas

II. IMPLEMENTACIÓN

II-A. Inicialización

II-A1. Disposición en memoria y carriles SIMD:

II-A2. Precálculo de constantes para división rápida:

II-B. Bucle principal

II-B1. Tabla de búsqueda optimista:

II-B2. Exponenciación modular de LSB a MSB:

II-B3. Núcleo $\alpha := \alpha m \bmod n$:

II-C. Interfaz de usuario

II-C1. Invocación:

II-C2. Visualización:

II-D. Resultados