Documentación de Implementación RSA

Jasson Rodríguez Méndez Marco Herrera Valverde Kenneth Hernández Salazar
Edgar Chaves González

Julio 2020

1 Plan de pruebas

La cobertura de pruebas del procesador debe ser lo más amplia posible con el fin de realizar una validación del funcionamiento esperado; además de representar una gran ayuda para la depuración y corrección de errores. Con el fin de obtener la mayor cobertura se realizaron pruebas unitarias; es decir, una prueba específica para cada una de las unidades funcionales implementadas. Además del funcionamiento unitario e individual es de suma importancia evaluar las interacciones de dichos componentes, para ello se implementaron pruebas de integración que consisten en pruebas sistemáticas que agrupan un conjunto de unidades funcionales y representan un submódulo del sistema final. Finalmente el sistema debe ser probado en su totalidad, como una sola unidad que hace uso de sus partes de forma armónica, en esta prueba se puede comprobar el resultado final del sistema y su correcto funcionamiento como un todo, para ello se implementó una única prueba de sistema que simula la agrupación y conexión de todos los componentes del procesador.

Al tratarse de un sistema de procesamiento de imágenes es muy complicado corroborar la validez del sistema mediante un análisis de señales pues es difícil de visualizar; además de tratarse de cantidades muy grandes de datos, para facilitar este proceso las pruebas que involucran la imagen escriben las señales de vídeo en un archivo de texto que es posteriormente visualizado con una herramienta externa.

2 Simulación de pruebas de sistema

En la figura 1 muestran las señales de mayor importancia que permiten analizar el comportamiento del procesador en modelsim.

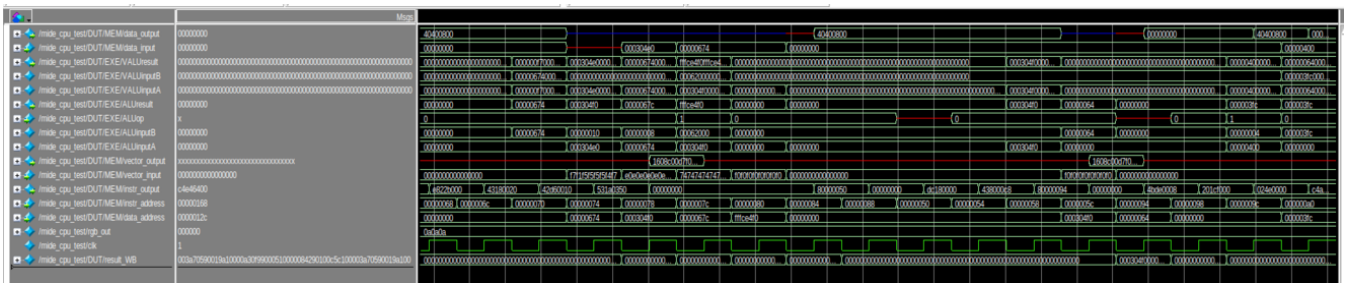

Figure 1: Vista de señales en modelsim para la prueba del sistema

El resultado final de dicha simulación se puede visualizar a partir del archivo que guarda las señales de vídeo, en este caso la simulación correspondiente a dos *frames* y por la configuración de la prueba, se puede visualizar la imagen encriptada y la desencriptada, como se aprecia en las figuras 2 y 3 respectivamente.

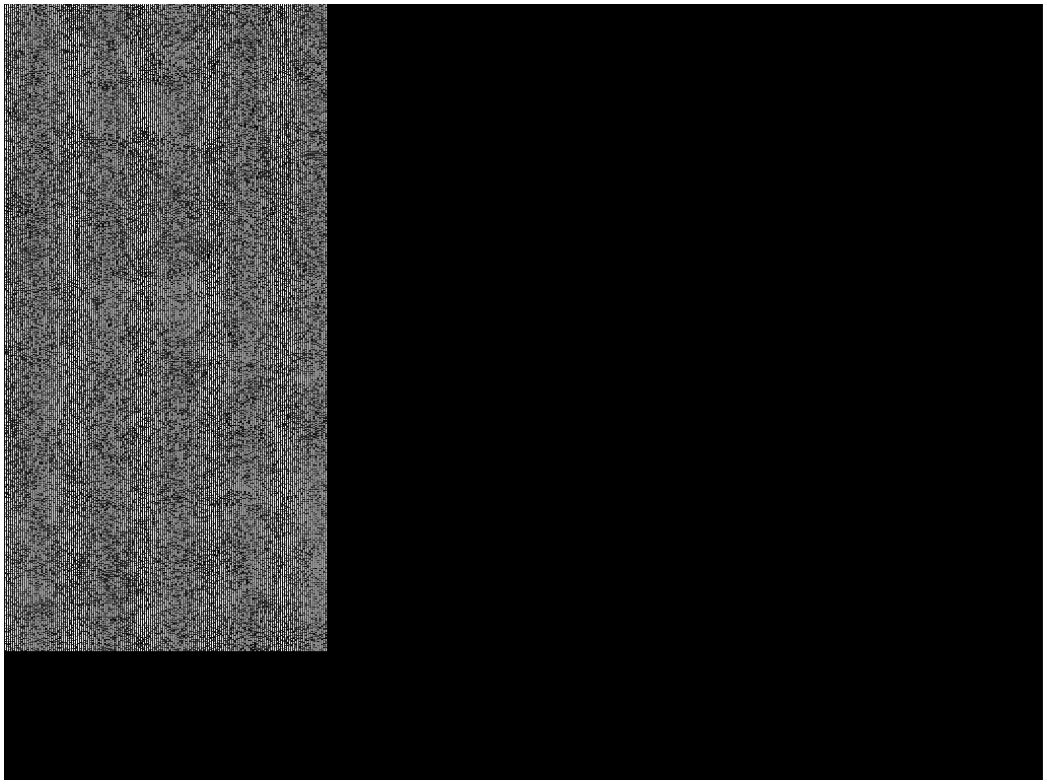

Figure 2: Vista de la imagen encriptada, resultado de la prueba del sistema

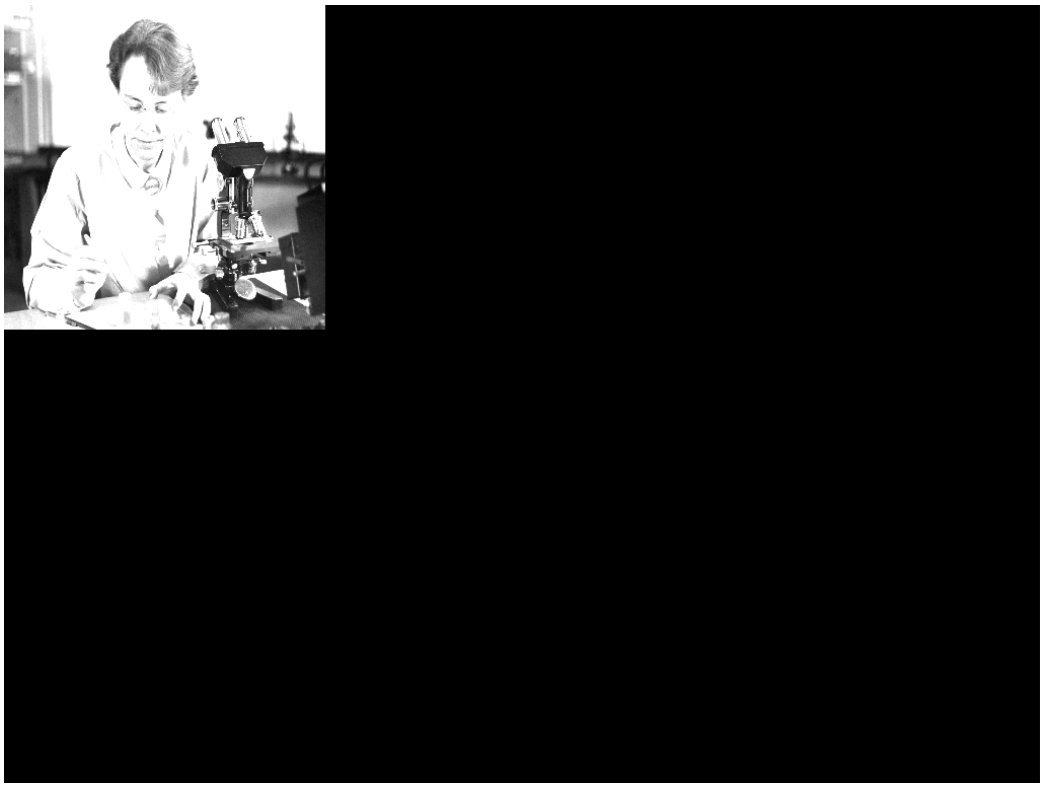

Figure 3: Vista de la imagen desencriptada, resultado de la prueba del sistema

3 Consumo de recursos

Para una futura implementación del procesador en un dispositivo FPGA se realizó el proceso completo de compilación de un archivo de tipo .sof específico que puede ser cargado directamente en una FPGA Altera DE1-SoC. En el proceso de compilación la etapa de *fitter* se encarga de enrutar todas las conexiones internas de la FPGA y verificar que existan los recursos necesarios para sintetizar el diseño. A continuación se presenta el reporte generado por el *fitter*:

Fitter Status : Successful - Wed Jul 15 17:46:06 2020
Quartus Prime Version : 20.1.0 Build 711 06/05/2020 SJ Lite Edition
Revision Name : mide_cpu
Top-level Entity Name : top
Family : Cyclone V
Device : 5CSEMA5F31C6
Timing Models : Final
Logic utilization (in ALMs) : 4,467 / 32,070 (14 %)
Total registers : 2023
Total pins : 30 / 457 (7 %)
Total virtual pins : 0
Total block memory bits : 2,928,640 / 4,065,280 (72 %)
Total RAM Blocks : 372 / 397 (94 %)
Total DSP Blocks : 9 / 87 (10 %)
Total HSSI RX PCSs : 0
Total HSSI PMA RX Deserializers : 0
Total HSSI TX PCSs : 0
Total HSSI PMA TX Serializers : 0
Total PLLs : 1 / 6 (17 %)
Total DLLs : 0 / 4 (0 %)