Sistemas en Chip acelerados por hardware: comparación de performance en aplicaciones criptográficas

Marcos J. Oviedo[1], Pablo A. Ferreyra[2,3], Carlos A. Marqués[1]

1: Facultad de Ingenieria – I.U.A,

2: Facultad de Ciencias Exactas, Físicas y Naturales –U.N.C.

3: Posgrado de Sistemas Embebidos – I.U.A.

Córdoba, Argentina

{esanchez, marques, ferreyra}@famaf.unc.edu.ar

Introducción

- Se demuestra una metodología de desarrollo de un HPSoC.

- Comparación de performance entre los resultados obtenidos de dos alternativas de implementación del algoritmo de encriptación simétrico (TripleDES).

Limitaciones de los sistemas basados en monoprocesador

- Concebidos para realizar computación de propósito general.
- No se puede aumentar la frecuencia arbitrariamente.
- Aumentar la cantidad de transistores introduce nuevos problemas de disipación de calor.
- Los procesadores tienen el limitante de la ejecución serial.

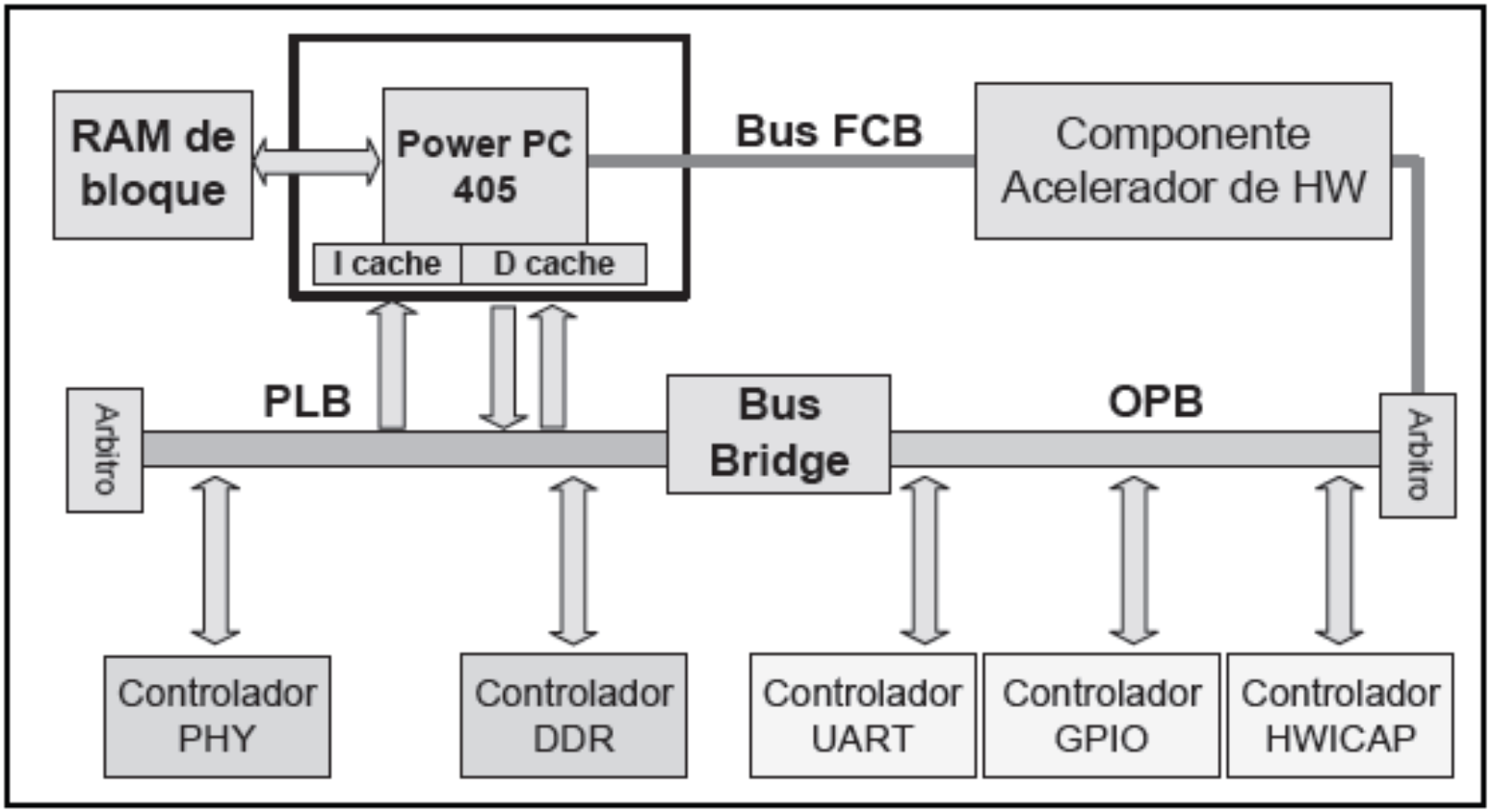
Metodología de desarrollo de un HPSoC

- Creación del soporte necesario para implementar un sistema embebido en la FPGA basado en microprocesador.
  - Ej: buses de interconexión, microprocesador, etc
- Optimización de la aplicación basada en un codiseño hardware-software.
  - Prototipo por software de la aplicación.
  - Determinar secciones críticas en términos de performance mediante *profilers*.
  - Refactorizar e implementar en *hardware.*

Optimización de performance en un diseño HPSoC

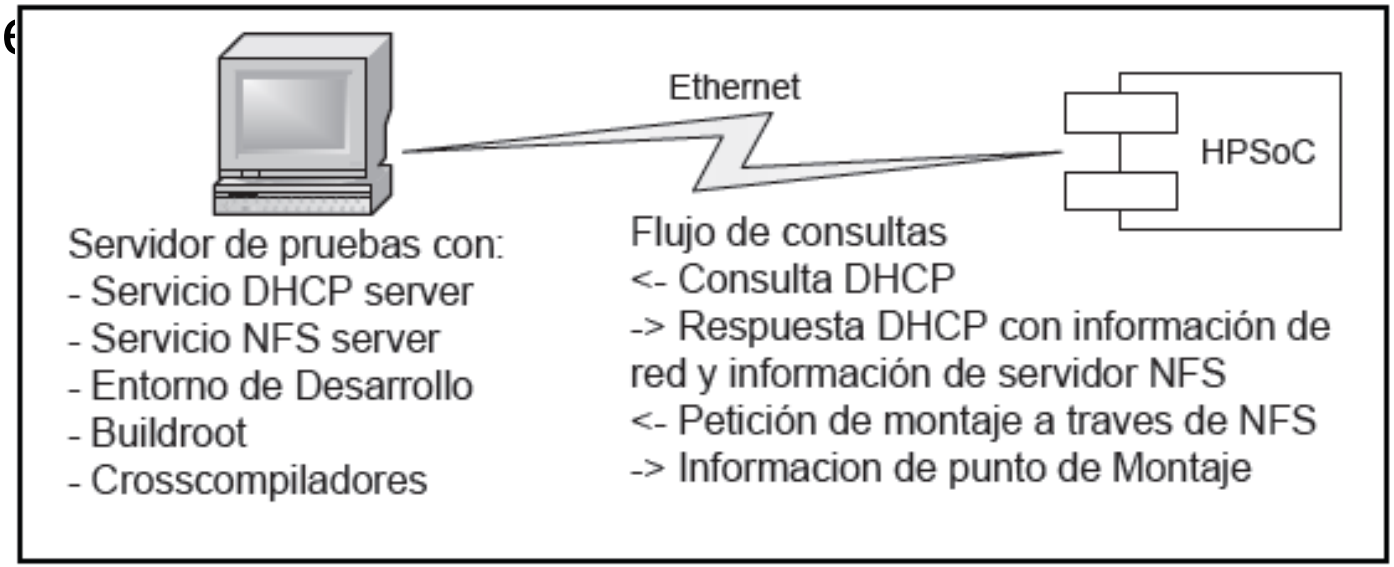
- Optimizaciones a nivel de Sistema
  - Buses de alta velocidad.
  - Caché
  - Restringir los tiempos en la síntesis.
- Optimizaciones a nivel de aplicación
  - Paralelismo, pre-cómputo de datos.
- Optimizaciones a nivel de micro arquitectura
  - Replicar los *arrays* para acceder en un solo ciclo de reloj.
  - Operaciones sobre bucles: si en cada iteración el set de datos es independientes, es alto el grado de paralelismo.

Desarrollo del HPSOC embebido



Desarrollo del *software* de control

- Linux: El kernel se ejecuta sobre el sistema embebido, se inicializa, detecta el *hardware* sobre el que se ejecuta, configurar las interfaces de red, autoconfigura su dirección de red a través de DHCP y boote



Resultados de implementación de HPSoC criptográfico

Implementación	**HPSoC TripleDES**		
	Frecuencia de operación	***Throughput (aplicación userspace)***	***Ganancia***
Software	300 Mhz	42.096 Kbps	1X
Hardware ImpulseC	50 Mhz	17.929 Mbps	415X
Hardware VHDL	50 Mhz	19.280 Mbps	458X