

UNA EXPERIENCIA EDUCATIVA: INTEGRACION DE PRACTICAS DESDE EL LABORATORIO DE ELECTRONICA DIGITAL HASTA EL DISEÑO VLSI

Diego V.J. SANTOS, Sadot ALEXANDRES y Juan M. MENESES

Departamento de Ingeniería Electrónica
E.T.S.I. Telecomunicación - Universidad Politécnica de Madrid
28040 - MADRID

Tfno: (91) 549 57 00 x 420
Fax: (91) 336 73 23
e-mail: dsantos@die.upm.es

RESUMEN

Se presenta una experiencia innovadora en la realización de prácticas de diseño digital en la E.T.S.I. Telecomunicación - Universidad Politécnica de Madrid. La misma abarca al laboratorio de electrónica digital, al laboratorio de microelectrónica y a la realización del proyecto fin de carrera (PFC). Se introduce a los alumnos en el diseño digital presentándoles un problema simplificado de cifrado de datos. A posteriori, en el laboratorio de microelectrónica, se plantea el diseño de un circuito VLSI que realice la misma función de cifrado, pero con especificaciones que permitan su empleo en sistemas de criptografía reales. Finalmente, en la realización del PFC se efectúa el diseño de un sistema completo de criptografía, que emplea como núcleo al chip VLSI realizado en el laboratorio anterior. Se consigue así pasar desde la etapa conceptual a la de diseño en un entorno profesional de VLSI, hasta la concepción e integración de un sistema empleando componentes desarrollados por el propio alumno.

1. INTRODUCCION

Con la experiencia que aquí se relata se busca dotar de contenido a las prácticas que el alumno va realizando, en el área de la electrónica digital, a lo largo de sus estudios. En repetidas oportunidades se ha cuestionado la poca relación entre lo enseñado y la tarea profesional. Mediante la integración y coordinación de los laboratorios y PFC se pretende ir dando a conocer aspectos sucesivamente más complejos del proceso de diseño, en analogía a lo que ocurre en los proyectos en un entorno industrial.

Asimismo, el problema de diseño planteado, cifrado de datos, tiene un campo de aplicación creciente y que despierta, por sus implicaciones, el interés de los alumnos. En resumen, se persigue:

- 1> Motivar al alumno al plantearle un problema que despierte su interés.
- 2> Plantear los trabajos como una sucesión natural de tareas cada vez más complejas, en lugar de como cuestiones aisladas.
- 3> Introducir al alumno gradualmente en el proceso de diseño, desde la resolución de un problema de interés exclusivamente didáctico, pasando por la especificación y diseño de un circuito VLSI que es enviado a fabricar, hasta la definición e implementación de un sistema completo.

Para ello se planteó la siguiente experiencia de integración de laboratorios. Se espera que los resultados ayuden a identificar el tipo de problema que motiva a los alumnos, y que permita enriquecer su formación.

2. LABORATORIO DE ELECTRONICA DIGITAL

El punto de partida es el laboratorio de electrónica digital, que forma parte del tercer curso. El laboratorio se desarrolla entre los meses de octubre y enero, y en él se busca que el alumno tome contacto por primera vez con los dispositivos usados en la implementación de circuitos digitales. Para eso se les plantea la construcción de un circuito que realiza una determinada función. Como apoyo se les da entre 2 y 3 clases preparatorias y se asignan los puestos de trabajo del laboratorio. Al finalizar el laboratorio se debe entregar una placa con el circuito funcionando.

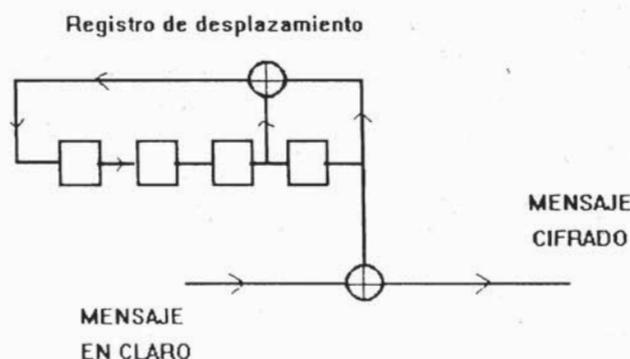


Figura 1. Cifrador continuo elemental

El problema propuesto fué la realización de un cifrador de datos continuo (stream cipher). Este consiste en un generador pseudoaleatorio de bits, los que son combinados en una función XOR con los datos del mensaje a enviar, figura 1. Se especificó para

realizar el generador pseudoaleatorio de bits un registro de desplazamiento con realimentación lineal (LFSR). En la placa debía disponerse de un almacenamiento para bits de mensaje, el LFSR para cifrado, y LEDs de siete segmentos para visualización del mensaje cifrado. Además debía incluirse el dispositivo inverso: LFSR para descifrado, y LEDs para visualizar el mensaje en claro. La simplificación didáctica consistió en especificar un LFSR de 4 bits. La secuencia pseudoaleatoria de bits de éste LFSR es tan pequeña que hace que carezca de utilidad práctica. Pero sirve para introducir a los alumnos en el tema del cifrado de datos, y la implementación alcanza una complejidad razonable para principiantes. También, en la idea de servir de estímulo, la relativa simplicidad del proceso de cifrado permitió plantear como cuestión adicional que los alumnos realizaran un ejercicio de criptoanálisis; es decir, intentaran determinar la forma en que un "espía" pudiera recuperar un texto en claro a partir de un mensaje cifrado, sin conocer la clave usada.

En la figura 2 se pueden ver las cantidades de alumnos que se han matriculado y se desglosan los resultados obtenidos. La evaluación del trabajo se hace teniendo en cuenta la calidad de los diseños y de la presentación de los mismos. Es de destacar el nivel de algunos trabajos, que llegaron a soluciones muy interesantes mediante el uso de recursos tales como memorias para mensajes, lógica programable (PALs), displays más complejos, placas de circuito impreso de muy buena calidad y presentación, etc. Casi la cuarta parte intenta resolver, además, el problema adicional que se les planteó.

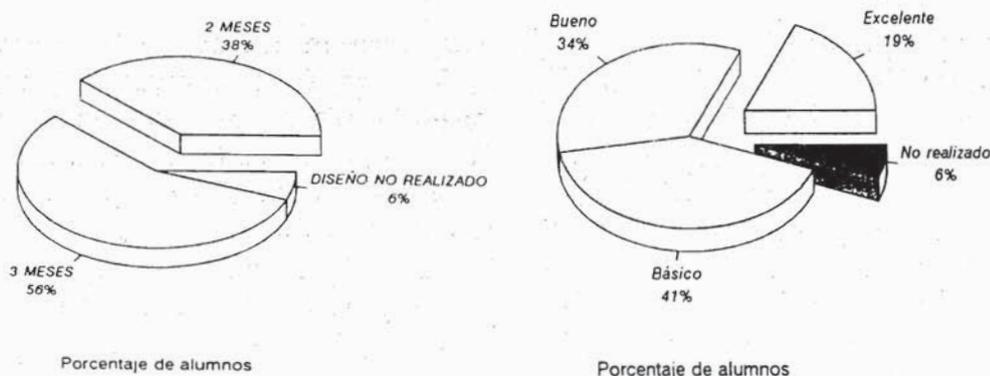


Figura 2. Resultados del laboratorio de Electrónica Digital

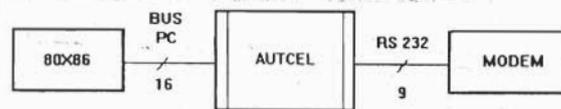
Se puede concluir que esta etapa demuestra ser una introducción adecuada a la técnica digital. Los alumnos responden muy bien y buena parte de ellos lleva al problema un paso más adelante, incorporando mejoras que no se exigen inicialmente.

3. DISEÑO VLSI

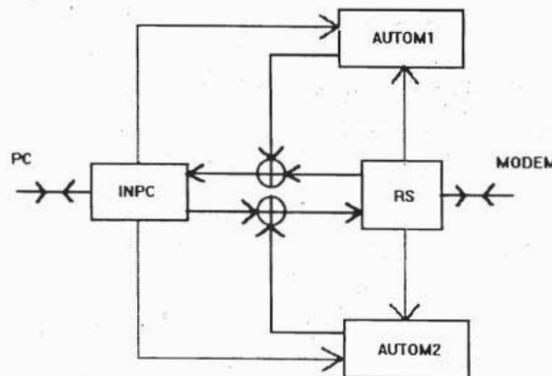
El laboratorio de microelectrónica pertenece al sexto curso, pero es realizado también por algunos alumnos en el quinto curso. Consiste en la realización de un ejercicio práctico de diseño VLSI empleando alguna de las herramientas disponibles

(SOLO 1400, Design Framework II, Synopsys, etc.). El resultado puede abarcar desde un simple informe de lo realizado hasta el envío a fabricación del diseño efectuado.

La siguiente etapa de la experiencia fué plantear, a un grupo reducido de alumnos del laboratorio de microelectrónica, el diseño de un circuito VLSI de cifrado continuo, a ser fabricado por medio del Programa EUROCHIP. La arquitectura del circuito en este caso estaba centrada en un generador de bits pseudoaleatorios muy innovador, empleando autómatas celulares [1]. El problema se presentó como trabajo previo al PFC, ya que las especificaciones del circuito eran para optimizar su empleo en un sistema cifrador de voz, para usarse en líneas telefónicas. El circuito a diseñar debía poder ser incluido en una placa de PC y conectado directamente a un modem. La arquitectura del circuito es la que muestra la figura 3. El circuito, AutCel, comunica con el procesador del PC vía el bus. Si bien la aplicación principal será con procesadores de la familia 80X86, para conservar cierta flexibilidad se exigió que parte de la lógica de interface no estuviera en el chip, sino en la placa externa. En el extremo opuesto se decidió no usar la salida serie del PC. La interface con el modem es directamente desde el chip. Para eso se debía incluir en el mismo la lógica completa que implementa una interface RS 232. Los bloques principales del circuito son: autom1 y autom2, generadores pseudoaleatorios de bits realizados mediante autómatas celulares; RS232, interface serie con el modem; Inpc, interface al bus del PC.



(a)



(b)

Figura 3. (a) Esquema del sistema de cifrado; (b) arquitectura del circuito integrado

El resultado de éste trabajo es un circuito integrado realizado con el entorno SOLO 1400 y librerías de ES2 de 1 micra. Durante el desarrollo de la práctica el alumno se enfrenta a un problema de diseño mucho más complejo que el del laboratorio anterior. Debe acostumbrarse a trabajar empleando herramientas de CAD de nivel casi profesional. Igualmente, se ve sometido a la disciplina que exige el diseño VLSI estructurado y se ve obligado a tomar sus primeras decisiones de diseño motivadas por un equilibrio entre los recursos disponibles.

El tiempo que este laboratorio demanda es de unos 5/6 meses. En general resulta ser un desafío importante para los alumnos por el nivel de dedicación que exige. Pero también su naturaleza hace que la motivación de aquellos que lo acometen sea muy alta, y esto se refleja en los trabajos realizados.

4. PROYECTO FIN DE CARRERA

El proyecto fin de carrera completa la formación de los alumnos. En él se pretende una síntesis de lo aprendido en los cursos anteriores. En nuestro caso se ha planteado como la culminación de un proceso de aprendizaje práctico comenzado en el tercer curso. En la experiencia que se relata, el tema objeto del proyecto es esbozado al comienzo del quinto curso. Ello es así porque se empleará en su desarrollo el resultado del laboratorio de microelectrónica. Esta situación requiere de una planificación clara por parte de los tutores/profesores y un fuerte compromiso por parte de los alumnos.

El proyecto planteado consiste en el diseño de un cifrador full-duplex de voz para transmisión telefónica. Integrado mediante una placa en un PC, debe permitir su conexión directa al modem y alcanzar velocidades de transmisión de hasta 14,4 Kb/seg. El núcleo del proyecto es, como se ha dicho, el circuito diseñado durante el laboratorio de microelectrónica, que ha sido enviado a fabricar. Pero con esto sólo se ha hecho una definición básica del sistema. En el curso del proyecto es necesario el esfuerzo de síntesis, que en este caso incluye, por ejemplo, la realización de funciones de digitalización y filtrado de la voz, compresión, integración del sistema. Todo ello obliga a considerar globalmente el proyecto, con aspectos tanto de hardware como de software. Es responsabilidad del tutor/profesor hacer énfasis siempre en las consideraciones de costo y facilidad de uso, obligando a pensar el sistema como si fuese un producto a ser lanzado al mercado.

El resultado de este trabajo debe ser el montaje, la prueba y la depuración del sistema completo, cerrando el ciclo con la elaboración de la documentación.

5. DISCUSION

A continuación se analizan algunos de los aspectos relevantes de la experiencia. Para comenzar, digamos que el esfuerzo requerido al tutor/profesor responsable del proyecto es grande. Ello impide la integración de los laboratorios en forma masiva, para todos los alumnos. El esfuerzo debe ser selectivo necesariamente, dividiendo a los alumnos en dos grupos con distinto grado de intensidad. La cantidad de alumnos

admitidos al grupo intensivo podrá ampliarse en función de la disponibilidad de profesores/tutores, evidentemente.

La dedicación que se demanda de los tutores está básicamente centrada en el esfuerzo de planificación del trabajo a realizar. Debe tenerse en cuenta que se toma un compromiso para dos años aproximadamente. Debe estar lo más claro posible el problema planteado, así como debidamente acotado su alcance.

Los alumnos deben saber desde el comienzo el tipo de dedicación que necesitarán. Sólo quienes tengan claro la tarea que van a acometer evitarn frustraciones y desiluciones al cabo del tiempo. Pero es de resaltar que pocas cosas dan tanta satisfacción a un alumno durante su carrera como tener en sus manos un circuito integrado diseñado por el mismo.

Finalmente, no se puede pasar por alto la necesidad de contar con infraestructura que permita soportar los proyectos planteados. Nos referimos a la necesidad de contar con las herramientas de diseño adecuadas, con equipo para montaje y depuración de hardware en el laboratorio y, desde luego, acceso a silicio a costos razonables en el caso de VLSI.

6. CONCLUSIONES

Creemos que con el esquema de integración de laboratorios y PFC esbozado se consigue un mejor aprovechamiento de las prácticas. El alumno va capitalizando las tareas realizadas, porque le sirven de base a las siguientes. El tema elegido permite estimular la creatividad y despertar el interés, lo que es tan importante como la mera transmisión de conocimientos. El campo de la electrónica digital proporciona gran cantidad de temas que pueden abordarse con el mismo método, desde una simplificación estimulante hasta el diseño de un sistema práctico. Finalmente, el pensar en términos de costo y sistema global deja lecciones que serán seguramente aprovechadas en la vida profesional.

7. BIBLIOGRAFIA

[1] S. Wolfram. "Cryptography with cellular automata". in *Proceedings CRYPTO '85*, Lecture Notes in Computer Science # 218, Springer Verlag, 1986, pp.429-432.