Cinvestav

26

Centro de Investigación y de Estudios Avanzados del Instituto Politécnico Nacional | Vol. 26, Núm. 02 | Abril - Junio 2007

COMPUTACIÓN
TECNOLOGÍAS DE LA INFORMACIÓN

Cinvestav

IEEE

ELECTRON DEVICES SOCIETY

iceee 2007

2007, 4th International Conference on Electrical and Electronics Engineering (ICEEE)

Mexico City, Mexico
Septiembre 5-7, 2007

Technical areas will include Topics on

Bioengineering and Medical Electronics
Biomedical Engineering
Communications Systems
Computers Science
Solid-State Electronics and VLSI
Mechatronics and Automatic Control
Electronics Circuits
Semiconductor Materials
Electrical Power

INFORMATION
M. en C. Judith Esparza Azcoitia
Departamento de Ingeniería Eléctrica CINVESTAV-IPN
Avenida Instituto Politécnico Nacional No. 2508, Col. San Pedro Zacatenco
Delegación Gustavo A. Madero, CP 07360 México, D. F., México
Phone: 52 (55) 50-61-38-00 Ext. 6503, 6505 Fax: 52 (55) 50-61-39-76
E-mail: iceee@cinvestav.mx http://iceee.ie.cinvestav.mx

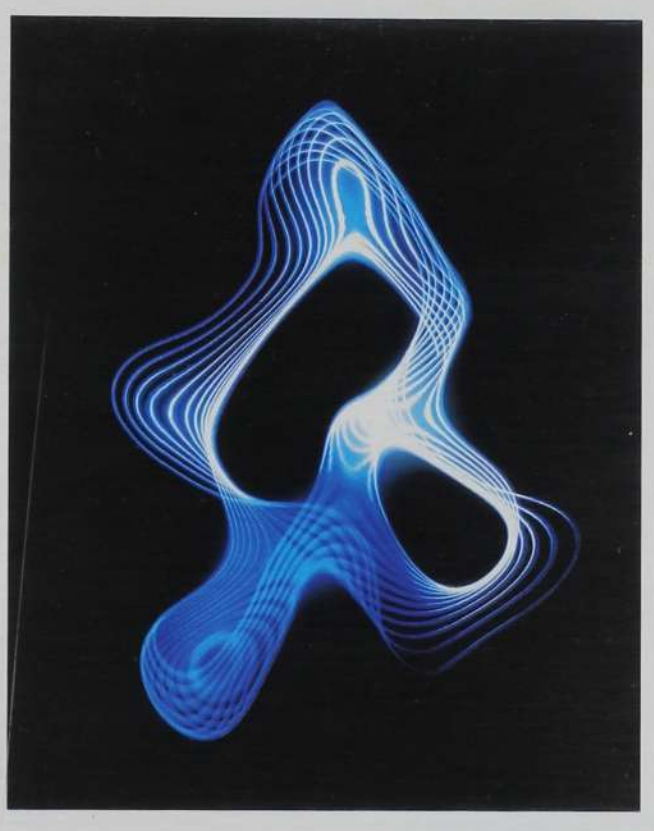
Full Manuscript: May 21, 2007
Review Notification: June 29, 2007
Final Revised Manuscript: July 30, 2007

This Conference is organized by the
Electrical Engineering Department
at Cinvestav-IPN Zacatenco http://cinvestav.mx

Head of the Electrical Engineering Department
Dr. Ernesto Suaste Gómez http://www.ie.cinvestav.mx

Cinvestav

abril-junio 2007



COMPUTACIÓN
TECNOLOGÍAS DE LA INFORMACIÓN

Contenido

Editorial
Luz Manuel Santos Trigo 3

El Departamento de Computación del Cinvestav
Carlos Artemio Coello Coello 4

El Laboratorio de Tecnologías de Información en Ciudad Victoria, Tamaulipas
Arturo Díaz Pérez 14

El Grupo de Ciencias de la Computación en el Cinvestav Guadalajara
Félix Francisco Ramos Corchado 28

Computación cuántica: un esbozo de sus métodos y desarrollos
Guillermo Morales-Luna 42

De la búsqueda de funciones booleanas con buenas propiedades criptográficas
Francisco Rodríguez Henríquez 50

El origen del miedo a las computadoras
Carlos Artemio Coello Coello 68

Vladimir Kharitonov, once años en México
Sabine Mondié Cuzange 72

Reseña
Cryptographic Algorithms on Reconfigurable Hardware
Miguel Ángel León Chávez 76

Noticias Cinvestav 78

La revista *Cinvestav* antes *Avance y Perspectiva*, órgano oficial del **Cinvestav** (Centro de Investigación y de Estudios Avanzados) es una publicación trimestral dedicada a la difusión y divulgación de la actividad científica y de la vida académica del Centro. Los artículos publicados son responsabilidad de sus autores. Se autoriza la publicación parcial o total del material publicado con el requisito de que se cite la fuente. La edición correspondiente a abril-junio 2007, volumen 26, número 2 se terminó de imprimir en junio de 2007. Tiraje: 5000 ejemplares. Certificado de Reserva de Derecho de Autor 04-2006-051210075200-102, expedido por la Dirección General de Derechos de Autor de la Secretaría de Educación Pública. Certificado de Licitud de Título 13538 y Certificado de Licitud de Contenidos 11111, otorgados por la Comisión Calificadora de Publicaciones y Revistas Ilustradas de la Secretaría de Gobernación. ISSN 1870-5499. Negativos, impresión y encuadernación: Lito Laser S.A. de C.V., Primera Privada de Aquiles Serdán núm. 28, Col. Santo Domingo Azcapotzalco, CP 02160, Del. Gustavo A. Madero, México DF. Sede del **Cinvestav**: Av. Instituto Politécnico Nacional núm. 2508, Col. San Pedro Zacatenco, CP 07360, Del. Gustavo A. Madero, México DF. Web del **Cinvestav**: www.cinvestav.mx

Editorial

Los notables avances y disponibilidad de herramientas computacionales han influido directamente tanto en la manera de formular nuevos problemas como en los métodos y representaciones que resultan importantes para su solución. El uso de herramientas como Internet, teléfonos celulares, videoconferencias, u otras tecnologías digitales, no sólo ha facilitado la comunicación eficiente e instantánea alrededor del mundo; también ha generado nuevos caminos y retos relacionados con la selección, procesamiento e interpretación de la información. De ese modo, la reflexión sobre el impacto de las tecnologías digitales puede enfocarse, por un lado, en la perspectiva de la generación de condiciones favorables para el desarrollo y la producción de herramientas computacionales y, por otro, en los beneficios y retos que su uso masivo puede generar.

¿Cuáles son las perspectivas de nuestro país en el campo de la computación o tecnologías de la información y comunicación?, ¿por qué y cómo el desarrollo de tecnología ha permitido que países como India, China y otros sean proveedores de servicios y productores de manufactura en este mundo de la información?, ¿qué implicaciones económicas y sociales se vislumbran en una sociedad cada vez más dependiente de los desarrollos tecnológicos? y ¿qué reformas en el sistema educativo nacional son importantes para participar directamente en la generación de herramientas computacionales? La discusión de este tipo de preguntas implica analizar la incidencia y la relevancia del desarrollo de la tecnología en la producción del conocimiento y en la solución de problemas del mundo cotidiano.

El **Cinvestav**, una institución de vanguardia en la generación de conocimiento y la formación de recursos humanos, ha impulsado sistemáticamente el desarrollo del campo de la computación. En la Unidad Guadalajara se ha formado el Grupo de Ciencias de la Computación, en la de Zacatenco, lo que fue la Sección de Computación de Ingeniería Eléctrica se trasformó, en 2006, en el Departamento de Computación, y en la Unidad Tamaulipas se creó, ese mismo año, el Laboratorio de Tecnologías de Información. Esta visión de promover el estudio de la computación contribuye directamente en el desarrollo del país y permite participar en la generación de conocimiento y proyectos de avanzada. El empleo de herramientas computacionales moldea el trabajo en todas las disciplinas académicas y hace importante la comunicación y colaboración con los grupos de computación dentro y fuera del **Cinvestav**.

Este número de la revista ***Cinvestav*** contiene artículos que describen las líneas de investigación y las dinámicas de trabajo asociadas con los grupos académicos que operan en las diferentes unidades del **Cinvestav**; asimismo, figuran en esta edición los artículos que difunden los temas y métodos que sus autores utilizan en el trabajo de investigación. En general, en todos ellos se destaca la urgencia y la necesidad de impulsar el desarrollo de la computación en nuestro país, de tal manera que permita no sólo generar o producir nuevas tecnologías digitales, sino también ser un polo de atracción donde converjan proyectos de interés nacional e internacional.

Agradezco al Dr. Carlos Coello por el interés y trabajo mostrado en la coordinación de los contenidos de este número.

Luz Manuel Santos Trigo
msantos@cinvestav.mx

FE DE ERRATAS

continuación se presenta la aclaración de algunos datos y textos que se integraron erróneamente en el articulo "Procesamiento de señales magnéticas del corazón y el cerebro fetales", del Vol. 26, Núm. 1:

- El correo del autor es: davidgtz@cinvestav.mx
- Pie de figura 1 (pág 10). Distintos tipos de magnetómetros usados para estudios fetales. (Sup. Izq.) Sistema Cryoton: biomagnetómetro de un solo detector. Cryoton UK Ltd. (Sup. Der.) Sistema Magnes 1300c: biomagnetómetro de 67 detectores. 4-D Neuroimaging. (Inf.) Sistema SARA: biomagnetómetro dedicado para estudios fetales con 151 detectores. CTF Systems Inc.
- Pie de figura 3 (pág. 13). Monitoreo del ritmo cardiaco de un feto en la semana 33 de gestación utilizando señales de fMCG capturadas por un SQUID del sistema SARA. (Sup.) Sección de la señal combinada de mMCG y fMCG (fT vs. segundos). (Cen.) Señal de fMCG extraida. (Inf.) Ritmo cardiaco fetal (latidos por minuto vs. segundos).
- En la página 14, figura 5, las imágenes sin la elipse marcada van del lado izquierdo, y las marcadas con la elipse van del lado derecho.

El Departamento de Computación del Cinvestav

CINVESTAV TARDÓ 23 AÑOS EN CREAR SU PROPIO DEPARTAMENTO DE COMPUTACIÓN, ENTRE OTRAS RAZONES, DEBIDO A LA DIFICULTAD PARA CONSEGUIR RECURSOS HUMANOS EN NÚMERO Y CALIDAD SUFICIENTES, LO CUAL HA SIDO, POR MUCHO TIEMPO, UNA TAREA MUY DIFÍCIL DE LOGRAR EN MÉXICO.

Carlos Artemio Coello Coello

Hoy en día, la importancia de la computación en nuestras vidas es, sin lugar a dudas, incuestionable. Dicha importancia se refleja en una clara (y a veces hasta obsesiva) dependencia de las computadoras, y las diversas tecnologías relacionadas con ellas, que presentan investigadores de diferentes disciplinas e, incluso, un número cada vez mayor de estudiantes y público en general. El mundo moderno parece girar en torno al ritmo que las computadoras le imponen, como podemos constatar a diario cuando vamos a un banco, cuando compramos un boleto de avión, cuando pagamos con una tarjeta de crédito y hasta cuando realizamos tareas tan simples como encender nuestro automóvil.

Sin embargo, y por extraño que esto pudiera sonar, a un lugar como el **Cinvestav,** que es un centro de investigación de primer nivel, con amplio reconocimiento nacional e internacional, le tomó 23 años poder contar con un Departamento de Computación. Las razones son varias, aunque principalmente se relacionan con la dificultad para conseguir recursos humanos en número y calidad suficientes, lo cual ha sido, por muchos años, una tarea muy difícil de lograr en México.[1] En este artículo se proporcionarán algunos retazos de esta larga historia que, a pesar de todo, concluyó con un final feliz: el establecimiento del Departamento de Computación del **Cinvestav** en la Unidad Zacatenco.

Antecedentes históricos

Corría el año 1983, y la computación se erigía, cada vez con más fuerza, como una disciplina vital para el desarrollo científico y tecnológico de las naciones (en particular, las más desarrolladas). No en balde, la prestigiosa revista norteamericana *Time*, en su ejemplar del 3 de enero de 1983, dedicó su portada a la "computadora", la cual fue denominada "máquina del año", reemplazando al tradicional "hombre del año" (ver figura 1).

El **Cinvestav,** siendo una institución científica de primer nivel, no era ajena a la importancia de las computadoras. Según consta en [1], el Departamento de Fisiología fue el primero en contar con una minicomputadora, en 1969. El uso de esta computadora fue compartido con el Departamento de Ingeniería Eléctrica, que la utilizó para investigaciones relacionadas con control digital directo y control de centrales telefónicas. Asimismo, se utilizó para fines docentes.

CARLOS ARTEMIO COELLO COELLO En 1996 se doctoró en Ciencias de la Computación en la Universidad Tulane (Estados Unidos). Es Investigador 3-D y Jefe del Departamento de Computación del **Cinvestav**. Pertenece al Sistema Nacional de Investigadores, nivel 3, y es miembro de la Academia Mexicana de Ciencias. Ha publicado más de 180 artículos en revistas y para congresos internacionales con arbitraje estricto. Es coautor del libro *Evolutionary Algorithms for Solving Multi-Objective Problems* (Kluwer Academic Publishers, 2002), coeditor del libro *Applications of Multi-Objective Evolutionary Algorithms* (World Scientific, 2004) y autor del libro de divulgación *Breve historia de la computación y sus pioneros* (FCE, 2003). Sus publicaciones reportan más de 850 citas en el *ISI Citation Index*. Es editor asociado de las revistas *IEEE Transactions on Evolutionary Computation* (IEEE Press), *Evolutionary Computation* (MIT Press), *Journal of Heuristics* (Springer) y *Computational Optimization and Applications* (Springer).
ccoello@cs.cinvestav.mx

Figura 1. Fachada del edificio que alberga al Departamento de Computación del Cinvestav Zacatenco.

En 1983, el uso de las computadoras de todos tamaños (desde *mainframes* hasta microprocesadores) y un número cada vez mayor de proyectos en el área de Ingeniería Eléctrica hacían evidente que, tarde o temprano, la computación electrónica acabaría por reclamar un espacio propio dentro del **Cinvestav**.

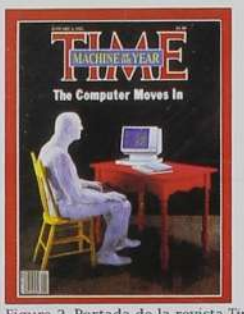


Figura 2. Portada de la revista *Time* del 3 de enero de 1983.

Para el año 1983, el **Cinvestav** contaba (según consta en [1]) con siete minicomputadoras, distribuidas en los Departamentos de Fisiología, Farmacología, Toxicología e Ingeniería Eléctrica. Asimismo, habían decenas de microcomputadoras y se tenía acceso a una computadora grande (*mainframe*) a través de diversas terminales. El Departamento de Ingeniería Eléctrica había estado impartiendo, desde 1972, cursos de computación electrónica, entre otros, Introducción a la computación, Teoría de autómatas y Arquitectura de computadoras. El uso de las computadoras de todos tamaños (desde *mainframes* hasta microprocesadores), en un número cada vez mayor de proyectos del Departamento de Ingeniería Eléctrica, hacía evidente que la computación electrónica acabaría por reclamar un espacio propio tarde o temprano.

Fue en esta atmósfera que se gestó una propuesta para establecer un Departamento de Computación en el **Cinvestav** hacia principios de 1983 [1]. Vale la pena reconocer los esfuerzos que realizaron los doctores Héctor Nava Jaimes (entonces Director General del **Cinvestav**), Juan Milton Garduño (entonces Jefe del Departamento de Ingeniería Eléctrica) y Adolfo Guzmán Arenas (fundador y primer Jefe de la Sección de Computación) para llevar a cabo esta empresa.

Debido a su valía histórica, es preciso rescatar los aspectos más sobresalientes de esta propuesta, los cuales serán discutidos brevemente a continuación [1].

- En la propuesta se plantean dos opciones posibles para dar un lugar propio a la computación dentro del **Cinvestav**:
  1) Contar sólo con un Departamento de Ingeniería Eléctrica y Computación.
  2) Contar con dos departamentos, el de Ingeniería Eléctrica ya existente y uno nuevo, el Departamento de Computación.

  En el documento se opta por planear la creación de un Departamento de Computación independiente del Departamento de Ingeniería Eléctrica, sin que esto, obviamente, implicara que la computación dejaría de cultivarse dentro del mismo. Una de las razones principales por las que se sugiere esta segunda opción es el tamaño que ya entonces tenía el Departamento de Ingeniería Eléctrica. Dado que se preveía que computación crecería bastante (debido a la importancia de esta disciplina), se argumentaba que tener juntos a los dos departamentos haría que en un periodo de dos o tres años, este departamento conjunto creciera al doble o al triple del tamaño que tenía en 1983 el Departamento de Ingeniería Eléctrica. También se daba el argumento académico. Puesto que las primeras licenciaturas en computación ofrecidas en México se remontan a finales de la década de 1960[2] [1], se argumentaba la necesidad de tener programas propios de posgrado en un Departamento de Computación que contaría, además, con una identidad específica.
- En la propuesta se planteaba una estrategia a tres años para la creación de un Departamento de Computación en el **Cinvestav**.
  1) Primer año: crear la Sección de Computación dentro del Departamento de Ingeniería Eléctrica.
  2) Segundo año: iniciar actividades como Departamento de Computación.
  3) Tercer año: formar al menos dos secciones del Departamento de Computación.
  Claramente, la propuesta indicaba la naturaleza transitoria que tendría la Sección de Computación, la cual se planteaba que iniciara operaciones en octubre de 1983. Según el cronograma incluido en la propuesta, para octubre de 1984 habría ya un Departamento de Computación funcionando en el **Cinvestav**. Evidentemente, esta meta no se cumplió, pues se requirieron 23 largos años para poder transformar la Sección de Computación en un Departamento de Computación.
- De acuerdo con la propuesta, en 1985 se tendrían al menos dos secciones dentro del Departamento de Computación, si bien la idea era contar con tres grupos de investigación, cada uno de los cuales tendría entre 10 y 15 investigadores, con una estructura jerárquica (por cada grupo de investigación habrían dos profesores titulares, tres o cuatro adjuntos, auxiliares de investigación y técnicos). Hacia comienzos del tercer año del proyecto se consideraba, en un cálculo conservador, que se contaría con al menos 12 investigadores (entre profesores titulares y adjuntos) y ocho auxiliares de investigación. También se planteaba iniciar el funcionamiento de una maestría en computación en octubre de 1983.
- Se estimaba que a partir de 1985 se formarían a 25 maestros en Ciencias de la Computación por año. Dato interesante, pues esta cifra ha sido alcanzada apenas en años recientes aunque, es importante mencionar, la Sección de Computación tuvo, desde su creación, la matrícula más alta de entre todas las secciones del Departamento de Ingeniería Eléctrica [6].
- Los objetivos del Departamento de Computación serían los de cualquier otro departamento del **Cinvestav**, es decir:

Las primeras licenciaturas en computación ofrecidas en México se remontan a finales de la década de 1960. Desde entonces, en el **Cinvestav** se fue haciendo más fuerte el argumento a favor de un Departamento de Computación autónomo, que tuviera programas de posgrado propios y una identidad específica, independiente del Departamento de Ingeniería Eléctrica, que le dio origen.

Figura 3. Cluster de 32 PCs ensamblado por personal del Departamento de Computación para fines académicos y de investigación.

1) Formación de recursos humanos.
2) Realización de proyectos de investigación que lleven al avance del conocimiento en el área.
3) Efectuar proyectos de desarrollo tecnológico que generen "objetos" (*hardware* y/o *software*) para resolver problemas prácticos específicos.
Estos objetivos no han perdido vigencia y siguen siendo los mismos del actual Departamento de Computación.

- Cabe destacar que el posgrado en computación ofrecido por la Sección de Computación fue uno de los primeros en México,[3] y el primero en ser ofrecido por un departamento de ingeniería eléctrica mexicano [6].

La separación de los programas de computación

Arturo Díaz Pérez hace ver en dos documentos, de 2000 [2] y 2001 [3], respectivamente, algunos de los altibajos que la Sección de Computación experimentó a lo largo de su historia. Por ejemplo, entre 1993 y 1997 no se superó la cifra de 10 graduados de maestría por año (muy por debajo de las cifras tan optimistas que se plantean en [1]). Sin embargo, es importante destacar que la planta de investigadores se mantuvo también reducida (entre 1996 y 1999 no se tuvieron más de ocho investigadores, incluso se llegó a un mínimo de seis en 1996).

En la historia de la Sección de Computación se puede hablar de cuatro etapas:

- **1983-1987**. Inicio de operaciones. Se realizan proyectos importantes con el Instituto Mexicano de Comunicaciones (de la Secretaría de Comunicaciones y Transportes), la UNESCO y la Gerencia de Telecomunicaciones de Pemex, entre otros. Cabe destacar que quedan pocos investigadores de ese periodo que todavía continúan apoyándonos en el actual Departamento de Computación: los Doctores Guillermo Morales Luna, Sergio Víctor Chapa Vergara y Ana María Martínez Enríquez.

Figura 4. Sala donde se alojan los servidores de red del Departamento de Computación.

Figura 5. Uno de los laboratorios de computadoras para uso de los estudiantes del Departamento de Computación.

- **1988-1992.** Crecimiento lento del grupo. Se gradúan unos 50 estudiantes de maestría y los dos primeros estudiantes de doctorado [2].
- **1993-1999.** Posiblemente, el periodo más crítico que hemos experimentado, ya que nuestros indicadores presentaron un descenso dramático, en buena medida debido al bajo número de investigadores disponibles.
- **2000-2006.** Periodo de consolidación en que nuestra planta de investigadores experimentó un crecimiento importante, el cual nos permitió alcanzar un punto de estabilidad en productividad académica y en nuestros indicadores.

A partir de 2002 fue cuando comenzó a vislumbrarse con mayor claridad la posibilidad de contar con los indicadores necesarios para hacer sostenible un programa de maestría y otro de doctorado, que fuesen independientes de los del Departamento de Ingeniería Eléctrica, así como la posibilidad misma de convertise en un departamento. Sin embargo, estas propuestas fueron vistas como actos de suprema osadía por varios miembros del Colegio de Profesores de aquel entonces, entre los que se incluye el autor de este artículo. Los escépticos cuestionaban la robustez de las buenas cifras, y pedían un poco más de tiempo para poder cerciorarse de que estos indicadores podrían ser sostenibles en el largo plazo.

Para 2005, los indicadores de la entonces Sección de Computación se mostraban ya bastante sólidos; finalmente se había alcanzado un periodo de estabilidad en lo concerniente a la productividad. Por ejemplo:[4] de los 12 investigadores de aquel entonces, 11 estaban en el Sistema Nacional de Investigadores (92%), la media de publicaciones en revistas internacionales con arbitraje estricto por profesor había sido superior a 2.0, el número de graduados de maestría por profesor era también superior a 2.0, la eficiencia terminal del programa de maestría superaba 50% y la de doctorado era muy cercana a 50%.

Es importante hacer notar que los buenos indicadores, que finalmente pudimos lograr como grupo, eran el medio para poder justificar ante Conacyt la separación de nuestros programas. Sin embargo, no constituían el fin en sí mismos, dado que la motivación principal para tal separación eran los problemas que nuestros estudiantes habían tenido en el pasado como consecuencia de egresar de un programa de Ingeniería Eléctrica. Al recibir un título que decía "Maestros en Ciencias" o "Doctores en Ciencias en Ingeniería Eléctrica",[5] los egresados solían enfrentar el escepticismo de algunos empleadores que llegaron a cuestionar si sus estudios realmente habían sido en computación. El hecho de ser una Sección del Departamento de Ingeniería Eléctrica, hizo también que nuestros programas aparecieran listados bajo esa disciplina en el padrón de excelencia del Conacyt, lo cual les restó visibilidad ante los (muchos) estudiantes que desconocían esta situación. Un ejemplo muy significativo de la poca visibilidad que la Sección de Computación tenía hacia el exterior es el estudio que realizó en 2002 la *Computing Research Association*, acerca de la investigación en México [8]. En este estudio se reconocían como grupos de desarrollo en computación los establecidos en CIMAT, CICESE, INAOE, LANIA, ITESM, UNAM, UDLA y CIC-IPN.[6] La Sección de Computación del **Cinvestav** no recibió mención alguna a pesar de que, en ese entonces, llevaba ya casi 20 años de existencia y los grupos referidos anteriormente sólo 10 [8].

Todo lo anterior motivó a que un grupo de investigadores de la citada Sección de Computación redactaran un plan para el establecimiento de programas de maestría y doctorado propios, independientes de los del Departamento de Ingeniería Eléctrica [4]. El documento fue sometido al Consejo Académico Consultivo (CAC) del **Cinvestav** en 2005. Tras estudiar nuestra propuesta, el Consejo recomendó, en 2006, que se autorizara la creación de ambos programas, pero con un carácter institucional a fin de que resultase más eficaz y ágil en lo referente al uso de los recursos humanos y materiales. En el dictamen emitido por el CAC se hace notar la indiscutible importancia que tiene la computación hoy en día, y se reitera que nuestra propuesta atendía uno de los programas prioritarios establecidos por el gobierno federal en su Plan de Desarrollo. Posteriormente, la Dirección General y la Junta Directiva del **Cinvestav** ratificaron esta decisión y quedó en nuestras manos someter el programa a la siguiente convocatoria del Programa Nacional de Posgrado (PNP) del Conacyt.

A pesar de que ello implicaría librar una guerra contra el reloj, se decidió, en un acto un tanto atrevido, someter nuestros programas a la convocatoria del 2006 del PNP. Preparar la documentación necesaria fue una tarea ardua que encabezó nuestro coordinador

En la historia de nuestra Sección de Computación se puede hablar de cuatro etapas, comprendidas entre los años 1983 y 2006, que dan cuenta de un lento crecimiento de los grupos de investigadores y estudiantes de maestría y doctorado, así como de sus crisis y logros en el camino recorrido hasta el 18 de septiembre de 2006, fecha en que se celebró la muy esperada fundación del Departamento de Computación.

Luego de una reciente revisión y actualización, las líneas de investigación del Departamento de Computación se extienden a cinco campos: fundamentos de la computación e inteligencia artificial; bases de datos y sistemas de información; programación de sistemas, sistemas operativos, sistemas distribuidos y sistemas de tiempo real; criptografía, arquitectura de computadoras y hardware reconfigurable y, finalmente, graficación, visualización y procesamiento de imágenes.

académico (Dr. Francisco Rodríguez Henríquez) y que pudo llevarse a buen término gracias a la valiosa ayuda de nuestras tres secretarias (Felipa Rosas López, Sofía Reza Cruz y Flor Córdova González). El esfuerzo valió la pena, pues nuestros dos programas (maestría y doctorado) fueron aprobados en la categoría de *Alto Nivel*.

La creación del Departamento de Computación

La separación de nuestros programas de maestría y doctorado llevó, de manera natural, a proponer la creación del Departamento de Computación. Las motivaciones fueron similares a las indicadas anteriormente, aunque en este caso se suma la independencia en el manejo presupuestal (considerado de gran importancia para poder definir políticas de desarrollo totalmente independientes de las de nuestros colegas del Departamento de Ingeniería Eléctrica), así como el deseo de tener una mayor visibilidad ante el resto del **Cinvestav**. Este interés nos llevó a presentar un nuevo documento en 2006, en el que se propuso la creación del Departamento de Computación [5]. El destino de este documento fue similar al de su predecesor: la propuesta se envió al CAC, el cual autorizó la creación del nuevo departamento. Posteriormente, esta decisión fue ratificada tanto por la Dirección General como por la Junta Directiva del **Cinvestav**. Para finales de agosto de 2006, el Departamento de Computación, así como sus dos programas propios de maestría y doctorado se hicieron realidad. Resulta más que evidente la euforia que nos invadió tras haber cumplido, en 2006, una meta que tomó 23 largos años en concretarse. El 18 de septiembre de ese año se realizó un brindis para celebrar tan importante evento, en el que se contó con la presencia de la Dra. Rosalinda Contreras Theurel (entonces Directora General del **Cinvestav**), el Dr. José Mustre de León (entonces Secretario Académico) y el Dr. Isidoro Gitler (Jefe del Departamento de Matemáticas), así como de un grupo numeroso de investigadores y estudiantes del recién creado departamento y del Departamento de Matemáticas.

En este punto vale la pena mencionar que la creación del Departamento de Computación no fue un fin en sí mismo para los investigadores que suscribimos esta propuesta. Más bien, preferimos ver la creación de este departamento como una etapa natural de evolución de un grupo de investigadores que requirió de varios años para consolidarse. Tal evolución ha sido práctica común en muchos otros lugares en México y en el mundo.

Indicadores actuales

Para dar mayor luz en torno a la situación actual del Departamento de Computación presentamos una serie de tablas que resumen nuestros indicadores principales. Cada una será brevemente discutida a continuación.

La tabla I muestra el número de estudiantes de maestría graduados por generación, en relación con el número de estudiantes que permanecieron activos (comúnmente existe un pequeño grupo de estudiantes en cada generación que deserta o reprueba cursos durante la maestría, por lo que nunca inician el trabajo de tesis).

Generación	Activos	Graduados	Porcentaje
2000	12	12	100%
2001	25	23	92%
2002	22	19	86%
2003	23	19	82%
2004	23	10	43%**
2005	23	N/A	N/A

Tabla I Estudiantes graduados por generación del programa de maestría. "Activos" son todos los estudiantes que iniciaron el trabajo de tesis. "N/A" significa "No Aplica", pues estos estudiantes todavía no cumplen los dos años de duración del programa de maestría. ** Los estudiantes no graduados de esta generación están todavía dentro del periodo de tres años que marca Conacyt como aceptable.

La tabla II muestra la eficiencia terminal lograda por cada generación de nuestro programa de maestría desde el año 2000. La eficiencia terminal se determina en la forma en que la mide Conacyt, es decir, con respecto a todos los estudiantes aceptados, y no sólo a los estudiantes activos (como se mostró en la tabla I). Puede verse que a partir de 2000 se ha logrado mantener una eficiencia terminal por arriba de 50%.

Hasta años recientes, nuestro programa de doctorado ha tenido un número bajo de estudiantes. Es por eso que muchos de los mecanismos de nuestro programa de doctorado se mantuvieron muy laxos en lo referente a los tiempos de graduación. La eficiencia terminal fue deficiente por varios años pero se ha hecho un esfuerzo importante por mejorarla. Últimamente se han implementado mecanismos más rigurosos para acortar los tiempos de graduación de doctorado. En la tabla III puede apreciarse que la eficiencia terminal de doctorado se ha mantenido también cercana a 50%, con un pico notable en la generación 2002, ya que logramos que 86% de esos estudiantes se graduara dentro de los

Año	Aceptados	Graduados	Porcentaje	Graduados en menos de 3 años	Porcentaje
2000	19	12	68%	10	53%
2001	32	23	72%	20	63%
2002	30	19	63%	16	53%
2003	26	19	73%	18	69%
2004	27	10	37%	10	37%**

Tabla II Eficiencia terminal de nuestro programa de maestría. ** Se hace notar que en este caso no se ha llegado al límite de tres años establecidos por Conacyt para los estudiantes de esta generación.

Año	Aceptados	Graduados	Porcentaje	Graduados en menos de 4.5 años	Porcentaje
2000	6	3	50%	3	50%
2001	5	3	60%	2	40%
2002	7	6	86%	6	86%
2003	5	1	20%	1	20%**

Tabla III Eficiencia terminal de nuestro programa de doctorado. ** Se hace notar que en este caso no se ha llegado al límite de 4.5 años establecido por Conacyt para los estudiantes de esta generación.

Año	Núm. de investigadores	Total en el SNI	Candidatos a investigadores	Nivel 1	Nivel 2	Nivel 3
2000	11	5	4	1	0	0
2001	11	5	3	2	0	0
2002	12	7	1	5	1	0
2003	12	9	1	7	1	0
2004	12	9	1	7	1	0
2005	12	11	1	9	0	1
2006	14	11	0	9	1	1

Tabla IV Número de investigadores que pertenecen al Sistema Nacional de Investigadores (SNI), así como su nivel correspondiente.

Año	Licenciatura	Maestría	Doctorado
2000	1	8	1
2001	2	7	1
2002	3	12	1
2003	6	12	0
2004	1	26	4
2005	0	30	7
2006	0	18	6

Tabla V Número de estudiantes graduados por año, incluyendo los niveles de licenciatura, maestría y doctorado.

Año	Núm. de cursos ofrecidos
2000	26
2001	29
2002	28
2003	25
2004	31
2005	30
2006	28

Tabla VI Número de cursos de posgrado (maestría y doctorado) ofrecidos por el Departamento de Computación cada año.

4.5 años que marcan los lineamientos del Programa Nacional de Posgrado del Conacyt. Un aspecto que cabe destacar aquí es que el mantener tiempos más rigurosos de graduación (o sea más cortos) no ha redundado en un decremento en la calidad de las tesis producidas por nuestros estudiantes. De hecho, podemos decir con orgullo que, de 2002 a la fecha, varios de nuestros egresados de maestría y doctorado han sido galardonados con el Premio a la Mejor Tesis en Computación, que anualmente otorga la Asociación Nacional de Instituciones de Educación en Informática (ANIEI). Destaca el hecho de que, en 2005 y 2006, han sido egresados nuestros los que han obtenido el primer lugar en este importante certamen.

Un punto en el cual el Departamento de Computación ha mostrado un progreso muy importante en años recientes es el de la pertenencia de sus investigadores al Sistema Naconal de Investigadores (SNI). En la tabla IV se muestran los datos de 2000 a la fecha. Es de destacarse el hecho de que, para 2006, el grupo de computación del **Cinvestav**, pese a su reducido tamaño, contaba ya con un investigador de nivel 2 y un investigador de nivel 3.[7] Estos números pueden lucir bastante modestos si se comparan con los de otros departamentos de la institución, sin embargo, es importante recalcar que la computación es una disciplina joven en México, y por ello existe un número muy bajo de investigadores de esta área en los niveles 2

Año	Artículos en revistas internacionales	Capítulos en libros	Artículos en congresos internacionales	Artículos en congresos locales	Libros
2000	7	0	14	13	0
2001	7	1	23	13	0
2002	20	4	21	11	1
2003	21	1	36	31	1
2004	31	1	41	8	1
2005	21	6	45	14	1
2006	20	3	34	9	1

Tabla VII Publicaciones producidas anualmente por los investigadores del Departamento de Computación, incluyendo artículos en revistas internacionales indizadas, capítulos en libros, artículos *in extenso* en congresos internacionales, artículos en congresos locales y libros (tanto en inglés como en español).

y 3 del SNI (aunque no tenemos el dato exacto, estimamos que no hay más de ocho investigadores en computación con nivel 3 del SNI, ni más de 15 con el nivel 2). De tal forma, son por demás escasos los Departamentos de Computación de nuestro país que cuenten con investigadores en los niveles altos del SNI, como escasos son también los programas de computación vigentes en el PNP de Conacyt.

La tabla V muestra el número de estudiantes graduados por año, en cada uno de los tres niveles (licenciatura, maestría y doctorado). Vale la pena indicar que hacia finales de 1999 se habían graduado sólo siete estudiantes de doctorado de la Sección de Computación, pese a que ésta llevaba ya 16 años de existencia. Sin embargo, del año 2000 a la fecha se han graduado 20 doctores en Ciencias, lo cual prácticamente triplica lo logrado en los 16 años previos. También destaca el hecho de que en diciembre de 2006 graduamos al estudiante 250 (considerando tanto maestría como doctorado). Dado que tuvimos al graduado 150 en diciembre de 2002, esto indica que graduamos a 100 estudiantes en un periodo de cuatro años. Hacia finales de 1999, sólo se habían graduado 119 estudiantes (112 de maestría y siete de doctorado) en los 16 años de existencia de la entonces Sección de Computación.

El número de cursos de posgrado ofrecidos por año se muestra en la tabla VI. Ahí puede verse que hemos logrado mantener un promedio de aproximadamente 28 cursos por año.

Finalmente, tenemos el rubro de las publicaciones, el cual se detalla en la tabla VII. Aquí destaca el importante incremento logrado en las publicaciones en revistas internacionales a partir del 2002, que se mantiene en un promedio de 20 artículos por año. También es relevante el hecho de que nuestros investigadores han publicado un libro por año (en español o inglés) de 2002 a la fecha. Tal volumen de libros (particularmente en inglés, publicados por editoriales internacionales) es sumamente inusual en nuestro país.

Líneas de investigación

A raíz de la creación del Plan para el Establecimiento del Departamento de Computación [4] se hizo una revisión y una actualización de nuestras líneas de investigación, las cuales quedaron constituidas de la manera siguiente:

- **Fundamentos de la computación e inteligencia artificial.** Comprende los fundamentos teóricos de la metodología de la computación y los modelos de razonamiento usados para el desarrollo de sistemas inteligentes. El área de Computación Evolutiva, la cual se refiere al uso de sistemas bio-inspirados para la solución de problemas computacionales difíciles, se considera también parte de esta línea, si bien su orientación ha sido más hacia la optimización que hacia la inteligencia artificial.
- **Bases de datos y sistemas de información.** Comprende el desarrollo e integración de sistemas de *software* basado en la descomposición funcional y el desarrollo de herramientas de *software*. Dentro de esta área, y con un fuerte componente tecnológico, se considera el desarrollo de aplicaciones, protocolos y herramientas para sistemas Web. Esta área ha tenido gran impacto dentro del **Cinvestav** (por ejemplo, a través del desarrollo del sistema de control escolar que se usa en el Centro).
- **Programación de sistemas, sistemas operativos, sistemas distribuidos y sistemas de tiempo real.** Comprende el diseño y desarrollo de *software* para administrar los recursos de sistemas de cómputo y para desarrollar *software* de aplicación. Es de destacar en esta área la importancia cada vez mayor de los mecanismos de seguridad informática a nivel de computadoras y redes de computadoras, los cuales requieren tomar como base estrategias generales para integrar soluciones *ad hoc* para un problema específico.
- **Criptografía, arquitectura de computadoras y *hardware* reconfigurable.** Comprende el estudio, análisis y diseño de prototipos en *hardware* reconfigurable de algoritmos criptográficos, algoritmos para compresión/descompresión de información y algoritmos aplicados a visión por computadora. Como parte de esta línea de investigación se encuentra el *cómputo reconfigurable*, el cual se refiere al uso de dispositivos de *hardware*

reconfigurable que permiten construir soluciones *hardware/software* a problemas computacionales altamente demandantes.

- **Graficación, visualización y procesamiento de imágenes.** Comprende la integración de herramientas computacionales diversas para resolver problemas de visión computacional, procesamiento de señales/video y visualización. Un área dominante en esta disciplina es la de *sistemas empotrados*, esto es, el desarrollo de dispositivos que tienen componentes de *software* empotrados en *hardware*. Por ejemplo, dispositivos tales como teléfonos celulares, agendas personales digitales, reproductores de audio digital, grabadoras de video digital, sistemas de alarma, máquinas de rayos X y herramientas médicas láser. Todos requieren de integración de *hardware* y *software* empotrado.

Actualmente, el Departamento de Computación cuenta con una planta de 15 investigadores de tiempo completo.[8] Sin embargo, sería deseable llegar a por lo menos 20 investigadores en los próximos años, ya que existen líneas de investigación de gran importancia que no cultivamos actualmente por falta de especialistas en esas áreas (por ejemplo, diseño de compiladores). Cabe destacar que contamos con el generoso apoyo de investigadores del Departamento de Matemáticas, pues ofrecen cursos que nuestros estudiantes pueden acreditar en nuestro programa. Asimismo, compartimos frecuentemente cursos (mediante videoconferencia) con el grupo de computación de **Cinvestav** Guadalajara y con el recién creado Laboratorio de Tecnologías de la Información de Ciudad Victoria, Tamaulipas. Es importante señalar que hemos colaborado (y lo seguiremos haciendo) con colegas de las Secciones de Bioelectrónica, Mecatrónica y Comunicaciones del Departamento de Ingeniería Eléctrica, así como con diferentes departamentos del **Cinvestav** y de otras universidades y centros tanto nacionales (UNAM, UAM, IPN, CIMAT, CICESE y BUAP, entre otras) como internacionales (la Universidad Joseph Fourier, la de Tulane, la Politécnica de Cataluña, etcétera).

A manera de conclusiones

Hoy, los investigadores del Departamento de Computación trabajamos con renovados bríos, y nos mostramos optimistas ante nuestro futuro, sin que ello implique olvidar los compromisos que tenemos con nuestra institución. Por lo pronto, nuestras metas son modestas y conservadoras. Por ejemplo:

- Incrementar el número de solicitudes de ingreso a nuestro programa de maestría.
- Mejorar nuestra eficiencia terminal tanto en maestría como en doctorado.
- Incrementar el porcentaje de investigadores que pertenezcan al SNI y, de ser posible, mejorar el nivel de los que ya se encuentran en el mismo.

En resumen, nuestras metas en el corto plazo giran en torno a la consolidación de nuestros programas y de nuestro departamento. De lograrlo, esperamos poder contar, en unos años más, con programas que ostenten un *nivel internacional* en el PNP. Esto conllevaría, evidentemente, disponer de un grupo de investigadores con reconocimiento no sólo nacional, sino también internacional, así como con indicadores mucho mejores que los que actualmente tenemos. Confiamos en que, si nuestro grupo de investigadores mantiene su ritmo de trabajo actual, esta meta, que ahora luce lejana (si bien no inalcanzable), podrá conseguirse.

Agradecimientos

Agradezco los comentarios y la información proporcionada por los Doctores Arturo Díaz Pérez y Guillermo Morales Luna para la realización de este artículo.

[Notas]

[1] Para tener idea de la gravedad de este problema señalemos que en 1999 el Conacyt indicaba que existían sólo 150 doctores en computación (o áreas afines).

[2] Aunque el Instituto Politécnico Nacional comenzó a ofrecer, desde 1965, las carreras de Técnico en Computación Electrónica y Técnico en Mantenimiento de Equipos de Computación y Electrónica, la primera licenciatura en computación en México (Ingeniería en Sistemas Computacionales) la ofreció el Instituto Tecnológico y de Estudios Superiores de Monterrey en 1968 [9] (en [1] se afirma que inició en 1969, mientras que en [7] se cita el año de 1967).

[3] En 1965, el Centro Nacional de Cálculo (Cenac) del Instituto Politécnico Nacional creó la primera maestría en ciencias con especialidad en computación de México. En el proceso se contó con la colaboración del Dr. Harold V. McIntosh, quien todavía mantiene una estrecha colaboración con el Departamento de Computación del Cinvestav.

[4] Los datos siguientes se elaboraron con cifras de 2004.

[5] En el caso del título de maestría, se indicaba un subtítulo que decía "Opción Computación".

[6] CIMAT, Centro de Investigación en Matemáticas (Guanajuato); CICESE, Centro de Investigación Científica y de Educación Superior de Ensenada; INAOE, Instituto Nacional de Astrofísica Óptica y Electrónica; LANIA, Laboratorio Nacional de Informática Avanzada A.C.; ITESM, Instituto Tecnológico y de Estudios Superiores de Monterrey; UNAM, Universidad Nacional Autónoma de México; UDLA, Universidad de las Américas (Puebla); CIC-IPN, Centro de Investigación en Computación-Instituto Politécnico Nacional.

[7] Cabe mencionar que estos investigadores fueron contratados después de 1999.

[8] Para mayor información sobre el Departamento de Computación, nuestros investigadores y actividades, favor de visitar la siguiente página web: http://www.cs.cinvestav.mx

[Referencias]

[1] Anónimo. Propuesta de Creación del Departamento de Computación del CIEA del IPN. Etapa I: Sección de Computación. Documento presentado por el Departamento de Ingeniería Eléctrica, CIEA del IPN, 1983.

[2] Díaz Pérez, Arturo. La Sección de Computación: pasado, presente y futuro. Cinvestav, febrero 2000.

[3] Díaz Pérez, Arturo. La Sección de Computación: Informe de labores 2000-2001. Cinvestav, octubre 2001.

[4] Varios autores. Propuesta para el establecimiento de los programas académicos de posgrado en la especialidad de computación. Cinvestav, junio 2005.

[5] Varios autores. Plan para el establecimiento del Departamento de Computación. Cinvestav, marzo 2006.

[6] Escobosa, Arturo. El Departamento de Ingeniería Eléctrica. En María de Ibarrola, Pedro Cabrera, René Asomoza, Eugenio Frixione, Augusto García, Miguel Ángel Pérez Angón y Susana Quintanilla (eds.). *El Cinvestav. Trayectoria de sus Departamentos, Secciones y Unidades, 1961-2001*, pp. 189-197, Centro de Investigación y de Estudios Avanzados del IPN, México, 2002, ISBN 968-5226-13-X.

[7] Cantarell, Aquiles y Mario González (coords.). *Historia de la computación en México: una industria en desarrollo*. Colección Hombre Digital, México, 2000, ISBN 968-5215-01-4.

[8] Computing Research Association. Computer Science Research in Mexico. *Computing Research News*, 14 (4), 2002.

[9] Gonzales, C. A computer engineering degree in Mexico. En *Papers of the SIGCSE/CSA Technical Symposium on Computer Science Education*, pp. 48-52, ACM Press, New York, 1978.

Crear un laboratorio dedicado al estudio y desarrollo de las tecnologías de información en Tamaulipas representa al **Cinvestav** un gran desafío y también una gran oportunidad para avanzar en su modelo de desarrollo descentralizado, que se inició hace más de 20 años.

Acceso a las instalaciones de la Unidad Tamaulipas.

El Laboratorio de Tecnologías de Información en Ciudad Victoria, Tamaulipas

EN 2005, CON LA FIRMA DE UN CONVENIO DE COLABORACIÓN ENTRE EL GOBIERNO DEL ESTADO DE TAMAULIPAS Y EL **CINVESTAV**, SE ESTABLECIÓ LA CREACIÓN DE UN CENTRO DE INVESTIGACIÓN EN COMPUTACIÓN Y DISEÑO ELECTRÓNICO, A FIN DE IMPULSAR EL DESARROLLO ECONÓMICO E INDUSTRIAL DEL ESTADO CON BASE EN EL CONOCIMIENTO CIENTÍFICO Y TECNOLÓGICO, A TRAVÉS DE PROYECTOS Y PROGRAMAS DE INVESTIGACIÓN DE IMPACTO REGIONAL.

Arturo Díaz Pérez

El 19 de diciembre de 2005 se firmó el Convenio de Colaboración para el Impulso de la Ciencia y Tecnología en el Estado de Tamaulipas por parte del Gobierno del Estado y la Dirección General del Centro de Investigación y de Estudios Avanzados del Instituto Politécnico Nacional. Diez meses después, el 19 de octubre de 2006, se inauguró oficialmente el Laboratorio de Tecnologías de Información dependiente del **Cinvestav** en Ciudad Victoria. La ceremonia fue presidida por el Secretario de Educación Pública, Dr. Reyes Tamez Guerra, el Gobernador Constitucional del Estado de Tamaulipas, Ing. Eugenio Hernández Flores y la Dra. Rosalinda Contreras Theurel, Directora General del **Cinvestav**.

El convenio de colaboración establece el interés de ambas partes en la creación de un centro de investigación en computación y diseño electrónico, a fin de impulsar el desarrollo económico e industrial del estado de Tamaulipas con base en el conocimiento científico y tecnológico, a través de proyectos y programas de investigación de impacto regional.

A catorce meses de la firma del convenio, muchas actividades se han realizado y muchas otras están pendientes o en proceso de desarrollo. Durante el primer semestre del año 2006 se buscó tener la infraestructura física básica para el establecimiento del Laboratorio de Tecnologías de Información, así como el equipo de trabajo necesario para el arranque de operaciones. El mes de julio de 2006 marcó el inicio formal de actividades de la nueva sede del Programa Institucional en Computación del **Cinvestav**, comenzando con el proceso de admisión a la maestría.

Actualmente, dicho laboratorio cuenta con siete investigadores y una primera generación de 16 estudiantes del programa de maestría. En las instalaciones provisionales se encuentran 12 oficinas para investigadores, áreas de trabajo para 60 estudiantes y dos aulas, cada una para 25 personas. Dada la naturaleza de los trabajos realizados en el laboratorio, por el momento basta disponer de una red de telecomunicaciones eficiente para aprovechar la infraestructura científica y tecnológica que posee el **Cinvestav** en sus diferentes sedes y unidades. Se está trabajando en el proyecto ejecutivo para la construcción de las instalaciones definitivas, lo cual será realizado por el Gobierno del Estado de Tamaulipas.

Mi participación en dicho proyecto empezó en enero de 2006. En el tiempo recorrido desde entonces, me he

ARTURO DÍAZ PÉREZ Doctor en Ciencias por el Centro de Investigación y de Estudios Avanzados del Instituto Politécnico Nacional (1998). Investigador **Cinvestav** 3A adscrito al Departamento de Computación; comisionado en el Laboratorio de Tecnologías de Información en Ciudad Victoria (Tamaulipas), donde funge como el responsable del proyecto. Coordinador General de Servicios de Cómputo Académico (2001-2006). Jefe de la Sección de Computación (2000-2001). Pertenece al Sistema Nacional de Investigadores. Entre sus intereses de investigación se encuentra el diseño de algoritmos paralelos para aplicaciones científicas, el diseño de algoritmos y arquitecturas para cómputo reconfigurable mediante el uso de dispositivos electrónicos programables. Es coautor de un libro dedicado a la implementación de algoritmos criptográficos en dispositivos reconfigurables. Ha dirigido tesis de licenciatura, maestría y, en codirección, una de doctorado. adiaz@cinvestav.mx

En un sentido amplio, el concepto de tecnologías de información puede entenderse como todo aquello que se relaciona con la disciplina de cómputo; en un sentido académico, hablamos de todas aquellas tecnologías que satisfacen las necesidades de automatización de información que requieren los negocios, el gobierno y las diversas organizaciones de los sectores salud, educación, entretenimiento, entre otros.

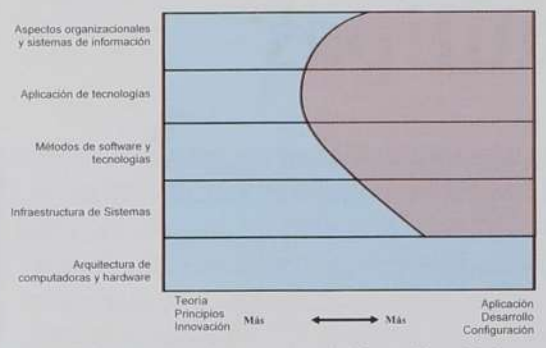


Figura 1. Niveles que cubren las tecnologías de información y énfasis entre teoría y aplicación (de acuerdo con [1]).

encontrado con algunas preguntas recurrentes –¿por qué tecnologías de información?, ¿por qué en Tamaulipas? y ¿por qué el **Cinvestav**?–, mismas que espero aclarar a lo largo de este documento. En la primera parte del escrito establezco el contexto del área de tecnologías de información en los ámbitos internacional, nacional y regional; en la segunda resalto algunos avances habidos en el proyecto del Laboratorio de Tecnologías de Información del **Cinvestav**.

Tecnologías de información

El término *tecnologías de información* se ha vuelto un referente importante en el mundo actual de la ciencia y tecnología, en la economía y en la sociedad en general. Está cada vez más presente en nuestra vida diaria; se menciona en los periódicos y noticiarios, y como tecnología aparece en nuestro hogar, en el trabajo y en los múltiples servicios nuevos que se nos van ofreciendo. Referirse a las tecnologías de información no sólo implica hablar de computadoras, sino también del uso y el desarrollo de programas de cómputo, de los servicios electrónicos (en empresas, organizaciones y dependencias de gobierno), de los medios electrónicos de comunicación no interactivos (correo electrónico y mensajería instantánea), de la comunicación interactiva (charlas en línea y videoconferencias), de la navegación por Internet y del acceso a bancos de información por medios alámbricos o inalámbricos, básicamente.

Las también denominadas *tecnologías de la información y comunicaciones* (TIC), dado que las comunicaciones se asocian con el transporte de la información, comprenden toda forma de tecnología usada para la gestión y transformación de la información, y, en particular, el uso de computadoras y programas que permiten crear, modificar, almacenar, proteger y recuperar esa información. Existen varias formas de presentar la información, por ejemplo, en forma de datos, conversaciones de voz, imágenes fijas o en movimiento, presentaciones multimedia, gráficos y otras. Las TIC están íntimamente relacionadas con computadoras, *software* y telecomunicaciones.

De acuerdo con la *Association for Computing Machinery* (ACM, por sus siglas en inglés) [1], el concepto de tecnologías de información tiene dos significados. En el sentido amplio, se refiere a todo lo que está relacionado con la disciplina de cómputo y, en el ámbito académico, implica todas aquellas tecnologías que satisfacen las necesidades de automatización de información que requieren los negocios, el gobierno y las diversas organizaciones de los sectores salud, educación, entretenimiento, entre otros. Sin embargo, a diferencia de los sistemas de información en donde el énfasis se establece sobre la información misma, en TIC el énfasis se hace en la tecnología más que en la información que transporta.

Los especialistas en tecnologías de información tienen una sólida orientación hacia la práctica que les permite desarrollar y configurar aplicaciones para organizaciones y personas de un espectro amplio. No obstante, dado que es necesario satisfacer las necesidades humanas en el uso de la tecnología de cómputo, la tecnologías de información se extienden también hacia la teoría e innovación a varios niveles, particularmente aquéllos que se refieren a las aplicaciones y al desarrollo de *software*. En la figura 1 se presenta un diagrama de las áreas que cubren las tecnologías de información y el lugar que ocupan dentro de las diferentes áreas de la disciplina computacional. En el eje de las ordenadas se describe el espectro que va desde la teoría, los principios y la innovación hasta las aplicaciones, el desarrollo y el aprovechamiento de la tecnología. También se presentan los diversos niveles a partir de los cuales se puede

Interior de las instalaciones de la Unidad Tamaulipas.

abordar la disciplina de la computación (para una explicación detallada del diagrama y de otras áreas de la disciplina computacional se recomienda revisar [1]).

La importancia de las tecnologías de información

El desarrollo de las TIC ha contribuido fuertemente a la formación de una nueva economía basada en el conocimiento. Las estructuras económicas han experimentado cambios trascendentes gracias a los avances tecnológicos, entre los cuales las comunicaciones y la informática destacan por haber revolucionado la velocidad en el intercambio de la información. El impacto de las TIC se ha extendido a todo tipo de actividades, desde el entretenimiento, trabajos académicos y gestiones gubernamentales hasta lo referente a las estructuras económicas. La incorporación de las TIC al ámbito de todo tipo de organizaciones hoy es, sin duda, uno de los pilares básicos para el desarrollo de un país.

En el nuevo paradigma tecnológico de la sociedad de la información, los gobiernos desempeñan un papel doble: son elemento tractor para la introducción y aplicación de las nuevas tecnologías, a la vez que promotores de políticas públicas orientadas a la expansión de las TIC en la sociedad. Los gobiernos deben servir como ejemplo e incorporar las posibilidades que las nuevas tecnologías, más eficaces y eficientes, ofrecen para prestar servicios a la sociedad, además de ser promotores de bienestar, premisa obligada para reducir la brecha digital entre los diversos sectores de la sociedad [2].

Área de trabajo para estudiantes.

Distintos gobiernos han establecido políticas públicas de largo plazo para el desarrollo de economías basadas en el conocimiento y con la intención de que la riqueza generada se distribuya entre amplios sectores de la sociedad. Países como España, Irlanda, India, Brasil y Corea del Sur, por citar sólo algunos ejemplos, han establecido programas de desarrollo de economías alrededor de las TIC. Es con 3 a 6% que la industria de tecnologías de información contribuye al PIB de cada uno de esos países. Está aquí el ampliamente citado caso de Bangalore (India), ciudad que en un poco más de 20 años convirtió la región aledaña, netamente agrícola, al sector de tecnologías de información más popular del mundo, con mil 850 compañías de desarrollo de *software* instaladas. Dicha industria emplea a más de 450 mil ingenieros especializados en desarrollo de *software* y se espera llegar a 2 millones de especialistas dedicados a este sector. El ingreso, producto de los servicios que se prestan en dicha industria, es de aproximadamente 23 mil millones de dólares anuales. Lo que es más notable es que el desarrollo de este sector promueve un efecto multiplicador sobre diversos sectores que proporcionan servicios adicionales para la industria y eso, finalmente, se traduce en bienestar de la población. El ejemplo de Bangalore ha demostrado que, en una economía cimentada en conocimientos, un programa de *software* vale en los mercados internaciones mucho más que toneladas de materias primas.

Los resultados de la India y otros países no son casuales. El mérito más importante es que sus economías se han basado en la educación y el conocimiento; en la preparación de especialistas con conocimiento profundo y de alto nivel en los diferentes ámbitos de las tecnologías de información. Estos desarrollos toman largo tiempo (más de 20 años para el caso de la India) pero los

Es ampliamente citado el caso de Bangalore (India), ciudad que en poco más de 20 años logró que la región aledaña, predominantemente agrícola, se convirtiera en el centro de tecnologías de información más popular del mundo: mil 850 compañías de desarrollo de *software* instaladas, 450 mil ingenieros empleados y una perspectiva de elevar el número de contratados a 2 millones; la industria genera aproximadamente 23 mil millones de dólares anuales.

resultados finales son sólidos y con un efecto de largo plazo. La lección que deja este ejemplo es que en la economía mundial actual, basada en la feroz competencia del libre mercado, la especialización y la profundización de conocimientos proporcionan una posibilidad de desarrollo para los países que toman como estrategia este tipo de iniciativas.

Las tecnologías de información en México

La cercanía de México con el principal consumidor de tecnologías de información del planeta, Estados Unidos, le representa algunas ventajas que otras regiones no tienen y que pueden ser aprovechadas para el desarrollo económico del país.

Aun cuando el sector de tecnologías de información y comunicaciones en México es demasiado reducido para competir internacionalmente y acceder a un mercado mundial, es importante el papel que juega y hay expectativas de que se convierta en un motor de la economía nacional. Según estimaciones de la Asociación Mexicana de la Industria de Tecnologías de Información (AMITI), si se llegan a dar las condiciones adecuadas, esta industria podría estar generando, en el ámbito nacional, 6 500 millones de dólares anuales, entre exportaciones y ventas internas, además de dar trabajo directo y bien remunerado a 300 mil profesionistas y técnicos [3].

En México, el sector de la informática participa con 3.5% del PIB total. Creció 27.2% en el año 2000 con respecto al año anterior, es decir, cuatro veces más que toda la economía en su conjunto. Del PIB informático, el sector que más creció (28.4%) fue el de telecomunicaciones, que representa 87% del total del sector, seguido de equipo y periféricos para procesamiento informático, cuyo aumento fue de 22.9%. Se estima que sólo el valor del mercado de *software* a nivel internacional crezca para el año 2009 en 27.5% con respecto al año 2004, situándose en unos 183.1 billones de dólares [4].

Ya desde el Plan Nacional de Desarrollo 1994-2000 se advertía sobre el papel fundamental de las TIC en el desarrollo económico. Sin embargo, en la edición de 2000-2006 se identificó a la industria de tecnologías de información y comunicaciones como un área de desarrollo estratégica, por lo que el Gobierno Federal estableció programas para su impulso. En el Programa Especial de Ciencia y Tecnología 2001-2006, el sector de TIC se reconoce como un área prioritaria, entre otras razones por su alta tasa de cambio científico y tecnológico, el impacto que puede tener en la población y en los sectores productivo y social, por su potencial de nuevos avances o desarrollos en el futuro mediato y por la oportunidad para la creación de empresas de base tecnológica y la elevación de su competitividad [5].

Por otra parte, en el sexenio 2000-2006 se estableció el Programa Nacional de Fomento a la Industria del Software, conocido como Prosoft [6]. Entre sus estrategias de desarrollo más importantes se encuentran las siguientes:

- Promover las exportaciones y la atracción de inversiones.
- Educar y formar personal competente en el desarrollo de *software*, en cantidad y calidad convenientes.
- Contar con un marco legal promotor de la industria.
- Desarrollar el mercado interno.
- Fortalecer la industria local.
- Alcanzar niveles internacionales en capacidad de procesos.
- Estimular la construcción de infraestructura física y de telecomunicaciones.

Ningún programa de desarrollo económico basado en el conocimiento puede tener éxito sin considerar el capital humano. Sólo como forma de comparación con el caso de la India presentamos, a continuación, algunas estadísticas provenientes de la ANUIES.

En el año 2004 había poco más de 654 mil estudiantes de nivel licenciatura en las diversas áreas de ingeniería y tecnología. De éstos, aproximadamente 202 mil realizaban estudios en áreas de computación y sistemas. Las carreras más concurridas en dichas áreas son la Ingeniería en Sistemas Computacionales y la licenciatura en Informática, con aproximadamente 75 mil estudiantes cada una. De hecho, considerando las dos carreras en un solo grupo, éste se ubicaría en el tercer lugar de las carreras de nivel licenciatura más pobladas, únicamente después de las licenciaturas en Administración y Derecho [7]. En el posgrado, la situación es muy diferente. De acuerdo con el Anuario

> Aun cuando el sector de tecnologías de información y comunicaciones en nuestro país es demasiado reducido para competir internacionalmente, la Asociación Mexicana de la Industria de Tecnologías de Información estima que, en condiciones adecuadas, esta industria podría generar 6 mil 500 millones de dólares anuales y emplear a 300 mil profesionistas y técnicos.

Estadístico 2004 de la ANUIES [8], en México había 19 mil 818 estudiantes de posgrado en las áreas de ingeniería y tecnología, de los cuales mil 694 hacían estudios de especialización, 15 mil 973 estaban en maestría y 2 mil 171 en doctorado. Para las áreas de computación y sistemas, los números son 644, 4 mil 815 y 303 estudiantes de especialización, maestría y doctorado, respectivamente. Sin embargo, sólo se reportaron 551 graduados de maestría y 26 de doctorado. Estas cifras reflejan la gran carencia de recursos humanos especializados en el área.

Las tecnologías de información en el estado de Tamaulipas

Varios gobiernos estatales realizan esfuerzos específicos que impulsan el crecimiento del sector de TIC con el fin de establecer una industria basada en el conocimiento. Ya sea en los planes de desarrollo o en los programas de ciencia y tecnología, en al menos ocho entidades federativas se menciona este sector como estratégico para el desarrollo económico regional [3]. Así, siendo el objetivo la activación económica y generación de empleos bien remunerados en las entidades, se busca aprovechar apoyos gubernamentales en esfuerzos conjuntos de gobierno, academia, iniciativa privada y organismos no lucrativos del sector.

Por otra parte, los reportes del Programa Prosoft, de la Secretaría de Economía, indican que en el año 2004 se habían constituido 11 agrupamientos (*clusters*) para el desarrollo de tecnologías de información en igual número de entidades; en 2005, la cifra alcanzó los 15 agrupamientos estatales y en 2006 se formaron otros 19 con el mismo propósito [9].

En su Plan de Desarrollo Estatal 2005-2010, el Gobierno del Estado de Tamaulipas ha establecido algunas directrices para el desarrollo de la ciencia y tecnología, así como para el crecimiento económico del sector de TIC [10]. Entre las más importantes destacan las que siguen:

- Fortalecer la infraestructura científica del estado y orientarla al crecimiento regional equilibrado.
- Impulsar la creación de grupos de investigación en las instituciones educativas ligados a empresas o grupos empresariales.
- Promover en las empresas la formación de grupos de investigación y desarrollo de tecnología ligados a instituciones educativas.
- Apoyar el equipamiento en empresas e instituciones públicas para el desarrollo científico y tecnológico.
- Desarrollar incubadoras de empresas especializadas en tecnologías de la información, autopartes, electrónica e industria del plástico.

Como puede observarse, el sector de tecnologías de información ligado a la investigación científica y tecnología se ha definido como prioritario en el desarrollo del estado de Tamaulipas.

En el *Reporte de potencialidades de las entidades para desarrollar núcleos de economía digital* (2002), la Secretaría de Economía hizo observaciones precisas sobre cada entidad federativa e identificó sus fortalezas y debilidades [11]. Se consideraron tres etapas de análisis: en la primera se evaluó el entorno con el fin de conocer las condiciones generales de cada entidad federativa; en la segunda se avanzó en un análisis cualitativo de las entidades que cuentan con un programa de desarrollo de la industria del *software* o que han manifestado su intención de elaborar un programa, y se evaluaron las fortalezas y debilidades de cada uno de los programas; finalmente, en la tercera etapa se identificaron algunas entidades que podrían adoptar un patrón del desarrollo del *software* en una perspectiva sectorial-regional.

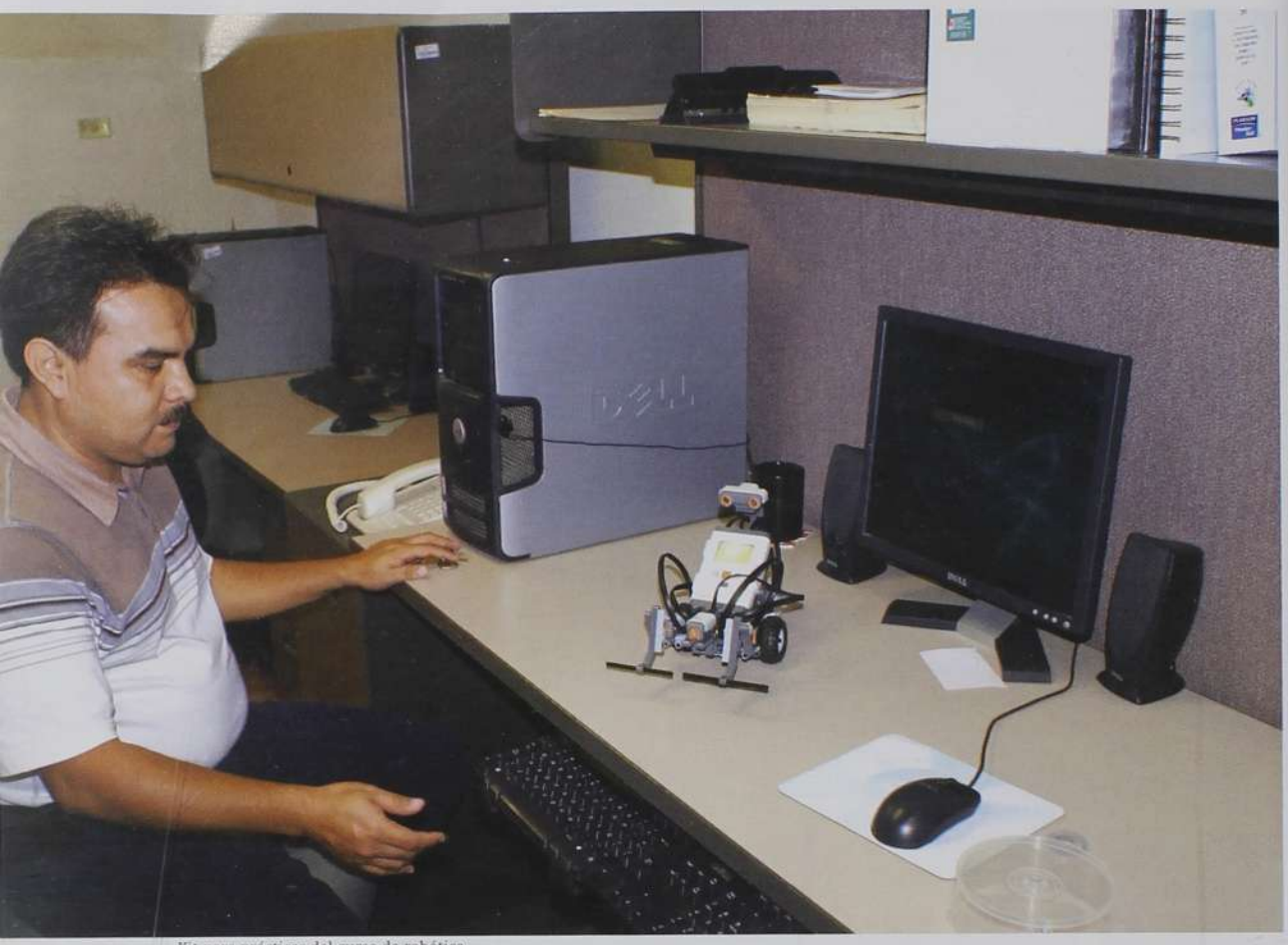
Para la primera etapa se establecieron seis indicadores que, sumados de forma ponderada, determinaron un índice de capacidades locales para cada entidad federativa. En el cuadro 1 se presenta el resumen de las capacidades locales para desarrollar núcleos de economía digital en las entidades federativas del noreste del país, comparadas con los valores obtenidos para el Distrito Federal (la región mejor ubicada) y con la media nacional. De las 32 entidades federativas, Tamaulipas ocupa el lugar 11, lo cual lleva a las siguientes conclusiones:

- La situación del estado es favorable (por encima del promedio nacional) en los indicadores para los núcleos de capital humano, de empresarialidad y de infraestructura para la economía digital.
- El índice que mide un entorno favorable está ligeramente por abajo del promedio nacional.
- El índice para el núcleo de aprendizaje e innovación es claramente inferior al promedio nacional. Tamaulipas ocupa el lugar 19 entre las 32 entidades federativas.

Dr. Víctor Jesús Sosa Sosa, investigador del Laboratorio de Tecnologías de la Información.

Entidad federativa	Índice de capital humano	Índice de aprendizaje e innovación	Índice de empresarialidad	Índice de entorno favorable	Índice de infraestructura digital	Valor de mercado	Índice de capacidades locales	Posición
D.F.	10.00	10.00	10.00	8.57	10.00	10.00	9.76	1
Nvo. León	9.68	7.74	8.37	7.80	7.57	9.68	8.46	2
Coahuila	8.97	4.86	6.40	5.60	7.44	6.77	6.66	6
Tamaulipas	7.94	3.13	6.48	4.73	8.03	6.45	6.11	11
Nacional	5.00	4.20	4.45	5.02	4.69	5.00	4.73	

Cuadro 1. Índice de Capacidades Locales de las Entidades Federativas [9].



Kit para prácticas del curso de robótica.

Información más detallada acerca del sector de tecnologías de información y comunicaciones en el estado de Tamaulipas se puede encontrar en [12].

El estado de Tamaulipas ha tomado varias iniciativas a fin de generar condiciones necesarias para el desarrollo de la industria de tecnologías de información. A la fecha del estudio (diciembre de 2002), el gobierno local no había elaborado un programa de desarrollo de la economía digital encaminado en esa dirección, pero en 2005, con el gobierno que inició actividades en ese año, finalmente se establecieron estrategias de desarrollo de la industria de *software* para el estado. La entidad ha redoblado sus esfuerzos para el desarrollo del capital humano, de tal manera que el nivel de educación promedio entre la población es de 8.1 años, contra 7.6 años a nivel nacional. Así también, Tamaulipas tiene cuatro de las diez instituciones de educación superior nacionales con el mayor índice de egresados en carreras relacionadas con computación y sistemas. Por otra parte, dada la cercanía con los Estados Unidos y la importancia que representa para el comercio del país, Tamaulipas ha creado una importante infraestructura para el desarrollo de la economía digital. En esta perspectiva, el estado posee una ponderación en el índice de capacidades locales por encima del promedio nacional. Claramente, es necesario realizar esfuerzos adicionales en materia de aprendizaje e innovación de nuevos procesos y productos, así como en la creación de un entorno favorable en la gestión de trámites empresariales e infraestructura telefónica. De acuerdo con los reportes más recientes del Índice de Capacidades Locales, en 2006 Tamaulipas avanzó dos posiciones y se sitúa en el lugar nueve de las 32 entidades federativas [9].

En 2005 se establecieron estrategias de desarrollo de la industria de *software* para el estado de Tamaulipas. Actualmente, la entidad tiene cuatro de las diez instituciones de educación superior nacionales con el mayor índice de egresados en carreras relacionadas con computación y sistemas.

La creación del Laboratorio de Tecnologías de Información en Ciudad Victoria

Como ya se mencionó en el inicio de este documento, en diciembre de 2005 se firmó el Convenio de Colaboración para el Impulso de la Ciencia y Tecnología en el estado de Tamaulipas entre el Gobierno del Estado y la Dirección General del **Cinvestav**. A partir del convenio se creó el Laboratorio de Tecnologías de Información (LTI) y se manifestó el interés en establecer un centro de investigación en computación y diseño electrónico. Veamos algunos pormenores de este proyecto.

Objetivos, planes y estrategias

La visión es tener un laboratorio especializado en tecnologías de información que contribuya al desarrollo científico y tecnológico de este sector en el estado de Tamaulipas, que funcione como detonador del sector de TIC en la región noreste del país y sea reconocido como tal en el ámbito mundial. Por lo anterior, la misión del proyecto es crear un centro de investigación con una unidad académica para la investigación científica y preparación de recursos humanos a nivel posgrado en tecnologías de información, así como una unidad de vinculación para el desarrollo de proyectos y programas de capacitación en el sector en la región del noreste del país.

Para este fin, un nuevo grupo de investigación está siendo adscrito al LTI ubicado en Ciudad Victoria. El objetivo del proyecto a cinco años es contar con 100 investigadores en las áreas relacionadas con tecnologías de información, que puedan atender a un total de 800 estudiantes de posgrado, maestría y doctorado, y que junto con el sector privado coadyuven al desarrollo de tecnologías de frontera en las áreas de desarrollo de *software*, telecomunicaciones y diseño electrónico. Es claro que desde el inicio se busca contar con un programa de posgrado acorde con los estándares de excelencia acostumbrados en el **Cinvestav**.

El modelo de operación de la Unidad Académica y la de Vinculación y Gestión Tecnológica, que se pretende establecer en el LTI, está sustentado en la experiencia de la Unidad Guadalajara del **Cinvestav**. Ambas unidades tendrán como enfoque principal el diseño electrónico, computación y telecomunicaciones.

La Unidad Académica tiene por objetivo realizar investigaciones científicas y desarrollos tecnológicos en las diversas áreas de tecnologías de información, como son: ingeniería, diseño y desarrollo de *software*, sistemas distribuidos, diseño digital, sistemas empotrados, seguridad informática, comercio electrónico y pruebas de *hardware* y *software*, entre otras. Por su parte, la Unidad de Vinculación y Gestión Tecnológica buscará desarrollar proyectos de diseño, construcción, mantenimiento y pruebas de sistemas de *software* en áreas de desarrollo tecnológico innovador. Se encargará, asimismo, del diseño de los cursos de capacitación y actualización, así como de su promoción.

A través de la sinergia entre la Unidad Académica y la Unidad de Vinculación, el LTI ofrecerá programas de especialización en computación, diseño electrónico, telecomunicaciones y diseño de *software*, con el fin de formar investigadores y profesionistas con un conocimiento profundo y amplio de la disciplina computacional y con la capacidad de generarlo. Adicionalmente, mediante esta relación estrecha se establecerán programas de capacitación de alto nivel a individuos y organizaciones que así lo requieran, aunado a servicios de consultoría y desarrollo tecnológico a empresas.

A fin de iniciar las operaciones del **Cinvestav** Tamaulipas a corto plazo, se ha planeado conformar un grupo de investigación de 10 especialistas en computación, con grado de doctor, el cual irá creciendo hasta llegar a 20 investigadores durante los primeros dos años. De acuerdo con los estándares de contratación de investigadores del **Cinvestav**, se buscará crear un cuerpo académico sustentado por algunos investigadores consolidados, que tengan una trayectoria científica bien identificada y sean miembros del Sistema Nacional de Investigadores (SNI). El cuerpo académico se completará con investigadores jóvenes, recién doctorados, con líneas de trabajo novedosas pero con un potencial claro para desarrollar una carrera académica exitosa. A los investigadores jóvenes se les pide que presenten su solicitud de ingreso al SNI en la primera convocatoria en la cual se tenga oportunidad. Por tanto, su perfil debe mostrar que tienen una alta probabilidad de ingreso, al menos en la categoría de candidato, y que podrán promoverse a nivel 1 en su primera renovación. Las

El objetivo del proyecto a cinco años, emprendido por el Laboratorio de Tecnologías de Información, es contar con 100 investigadores y 800 estudiantes de posgrado, además de coadyuvar al desarrollo de tecnologías de frontera en las áreas de *software*, telecomunicaciones y diseño electrónico.

áreas de trabajo que se han identificado como prioritarias, pero no limitadas, son: ingeniería y tecnología de *software*, sistemas de información y bases de datos, redes de computadoras, telecomunicaciones, sistemas distribuidos, diseño electrónico, sistemas empotrados, seguridad informática, computación evolutiva e inteligencia artificial.

En la primera etapa del proyecto, los programas académicos de maestría y doctorado están asociados al Programa Institucional de Computación del **Cinvestav**, el cual ha sido aprobado por la Junta Directiva de esta institución durante el año 2006 para ser desarrollado en sus diferentes sedes. Dicho programa, elaborado en la sede Zacatenco, también está reconocido como Programa de Posgrado de Alto Nivel en el Padrón Nacional de Posgrado de Conacyt. A los estudiantes admitidos al programa que cubren los requisitos de Conacyt, se les otorga una beca de manutención.

La computación es una de las partes fundamentales de las tecnologías de información, sin embargo, éstas tienen una connotación más amplia y diversa. En una segunda etapa, y una vez conformado el cuerpo académico, se realizarán las adecuaciones necesarias al programa de posgrado para ampliarlo y cubrir todas las áreas de tecnologías de información.

La Unidad de Vinculación Tecnológica se encargará del desarrollo de proyectos para el sector público y privado en el estado de Tamaulipas, con lo cual se apoyará científica y tecnológicamente a la industria informática y electrónica de la región. Así también, se apoyará al Gobierno del Estado en su estrategia regional de desarrollo de la industria de alta tecnología basada en TIC. Particularmente, se prestará asesoría en la etapa inicial de la conformación del *cluster* de tecnologías de información.

Situación actual

La iniciativa de creación del Laboratorio de Tecnologías de Información tiene catorce meses de desarrollo. A continuación se presentan algunos avances en la puesta en marcha del laboratorio.

Instalaciones provisionales

El laboratorio se ha instalado de manera provisional en el inmueble localizado en el kilómetro 6 de la carretera Cd. Victoria–Monterrey (frente al ejido Benito Juárez), con una extensión 12 mil 950 m^2 de superficie de terreno y un área construida de mil 529 m^2, con 900 m^2 de espacios útiles, que son los siguientes:

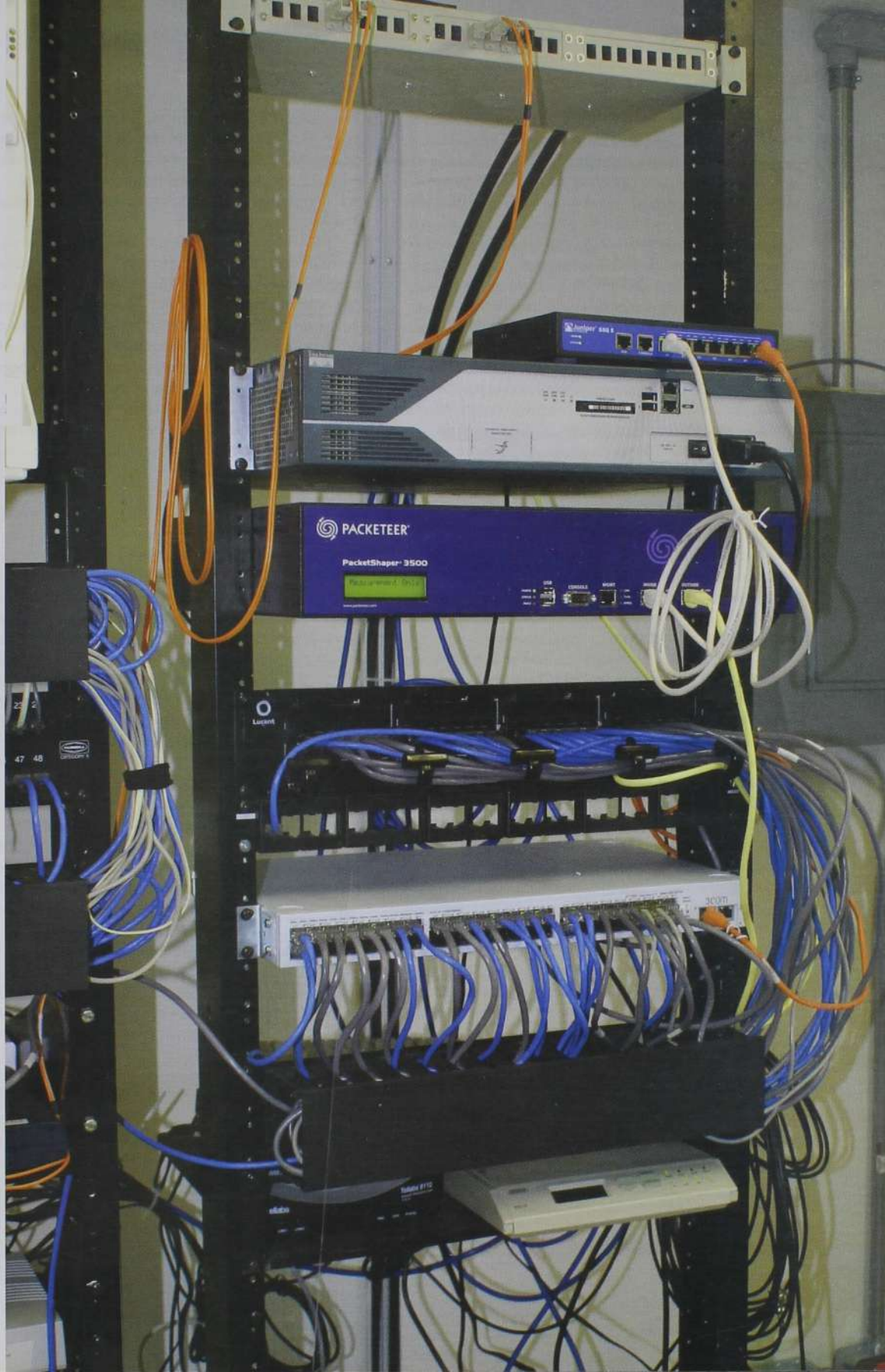
- Área administrativa que consiste de una recepción, una oficina del administrador, una oficina de la dirección y dos salas de usos múltiples.
- Un espacio reservado como *site* de telecomunicaciones.
- Doce oficinas reservadas para investigadores.
- Diez áreas de trabajo para seis estudiantes cada una.
- Sala de conferencias con una capacidad de 50 personas.
- Espacio habitacional de 13 cuartos.

Además de la remodelación de las instalaciones físicas, se colocaron redes eléctricas requeridas para el uso de las instalaciones, así como para los servicios de comunicación de voz y datos, y de telecomunicaciones que enlazan la sede Tamaulipas con todas las unidades del **Cinvestav**. Las instalaciones remodeladas cuentan ya con el mobiliario básico, adquirido en 2006, para atender a los ocupantes potenciales. Asimismo, se ha integrado todo el equipamiento necesario para comunicaciones por voz y datos, y se cuenta con el equipo de cómputo requerido para los servicios esenciales de comunicaciones y para todos los puestos de trabajo previstos.

Instalaciones definitivas

Se revisaron cinco propuestas de espacios territoriales para la construcción de **Cinvestav–Tamaulipas**. Después de analizar las ventajas y desventajas de cada propuesta, se eligió un terreno de 10 hectáreas para edificar las instalaciones definitivas, localizado al norte de Ciudad Victoria, a 15 minutos del centro de la ciudad. La localidad se integrará a un espacio territorial destinado a la construcción de un parque tecnológico a cargo del gobierno del estado.

A partir de los requerimientos de uso y tamaño de los espacios necesarios para **Cinvestav–Tamaulipas**, se tiene ya el diseño de la planta arquitectónica de las instalaciones definitivas. Consta de un conjunto de siete módulos repartidos en dos plantas, que albergarán


PACKETEER
PacketShaper 3500

cubículos de investigadores, laboratorios, aulas, áreas de vinculación, área administrativa, auditorio, biblioteca, cafetería y servicios de apoyo. Se está trabajando en el proyecto ejecutivo para definir el catálogo de conceptos y establecer el programa de construcción de los edificios.

Planta de investigadores

Al autor de esta comunicación le ha sido encargada la creación del LTI y, actualmente, en comisión académica por parte del Departamento de Computación, se ha integrado como uno de los investigadores de dicho laboratorio. Para conformar la planta de investigadores restante, se han recibido 32 solicitudes y se han realizado 14 entrevistas de trabajo, ya sea presenciales o por vía remota. Con la Dirección General se acordó la contratación de seis investigadores (ver el cuadro 2). Siendo el propósito iniciar en el año 2006 el programa de posgrado, se dio prioridad a investigadores de las áreas de computación. De la planta de investigadores actual, cinco provienen de esa área y dos tienen líneas de investigación relacionadas con el diseño electrónico o de dispositivos electrónicos. La estrategia para 2007 es cumplir con la plantilla de 10 investigadores, y para julio del año siguiente, la expectativa es contar con 20 de ellos.

Programa de posgrado

A partir de agosto del año 2006 se inició en la sede Tamaulipas el Programa de Posgrado Institucional de Computación del **Cinvestav**. La idea de un posgrado institucional es nueva en el **Cinvestav**, y el de computación es el único programa que tiene dicho perfil dentro de la institución. Este posgrado permite integrar a más investigadores al programa evitando la concentración y la oferta del mismo en un solo lugar geográfico. Es claro que esta idea puede no ser viable para cualquier disciplina, debido a la infraestructura científica que requiere un programa de posgrado. En el caso de computación, un mecanismo adecuado de colaboración y una infraestructura de telecomunicaciones estable permiten, sin importar la ubicación geográfica, que todos los investigadores participen en un solo programa de posgrado. Los siete investigadores adscritos al LTI están involucrados en la impartición de cursos y, en su momento, dirigirán tesis de grado.

A partir del mes de junio se inició el proceso de admisión al programa de maestría, que consistió en las etapas de difusión, examen de admisión, entrevistas con los candidatos, curso de inducción al posgrado y admisión definitiva. Al concluir este proceso, se tuvo un ingreso de 16 estudiantes.

En el periodo agosto-diciembre de 2006 se impartió el primer cuatrimestre del periodo académico y se ofrecieron cuatro cursos de posgrado de manera presencial en las instalaciones del LTI. Además, a través de videoconferencia se recibió el curso de graficación, impartido en el Departamento de Computación dentro del mismo programa de posgrado. En el cuatrimestre enero-abril del año 2007 se impartieron seis cursos de manera local y se tiene una colaboración para el curso Aritmética Computacional de dos investigadores, uno del Departamento de Computación y otro del LTI.

Vinculación

De acuerdo con los compromisos formulados en el Convenio de Colaboración, se establece la obligación de realizar actividades de vinculación con dos sectores importantes: las instituciones de educación superior y empresas del sector de tecnologías de información.

Aun cuando el inicio de actividades es relativamente reciente y el grupo de investigadores se encuentra en proceso de conformación y crecimiento, se han tomado algunas acciones para promover la vinculación del LTI con los sectores mencionados. Figuran, entre las más importantes, participación como jurado en certámenes locales, pláticas informativas en instituciones de educación superior de la región y conferencias magistrales, como las impartidas en el Congreso Internacional de Investigación en Computación 2006, organizado por el Instituto Tecnológico de Ciudad Madero, y en la reunión anual del Programa Prosoft celebrada en Ciudad Victoria los días 6 y 7 de noviembre de 2006.

Por otra parte, a invitación de la Secretaría de Desarrollo Económico y del Empleo se participó en la revisión del Estudio de Mercado del Sector de Tecnologías de Información en el Estado de Tamaulipas.

NOMBRE	CATEGORÍA	LÍNEAS DE INVESTIGACIÓN
Dr. Arturo Díaz Pérez	Investigador Cinvestav 3A	Cómputo reconfigurable, sistemas paralelos y distribuidos
Dr. Claudio Castellanos Sánchez	Investigador Cinvestav 2A	Redes neuronales
Dr. Iván López Arévalo	Investigador Cinvestav 2A	Inteligencia artificial
Dr. Víctor Jesús Sosa Sosa	Investigador Cinvestav 3A	Sistemas distribuidos
Dr. José Torres Jiménez	Investigador Cinvestav 3C	Optimización combinatoria e ingeniería de software
Dr. Gregorio Toscano Pulido	Investigador Cinvestav 2C	Computación evolutiva
Dr. Gabriel Ramírez Torres	Investigador Cinvestav 2C	Robótica

Cuadro 2. Investigadores adscritos al Laboratorio de Tecnologías de Información.

Se hicieron las observaciones y recomendaciones correspondientes en varias reuniones de trabajo sostenidas con los responsables del Cluster Tamaulipas de Tecnologías de Información, y se participó en la definición de estrategias para la planeación de su desarrollo.

¿Qué sigue?

A poco más de una año de su desarrollo, hay muchas tareas pendientes para el avance del Laboratorio de Tecnologías de Información. Tomando en cuenta los compromisos establecidos en el Convenio de Colaboración, se mencionan de manera general las actividades del laboratorio que son prioritarias para su futuro inmediato:

- Fortalecimiento de la planta de investigadores (el núcleo del desarrollo del laboratorio está basado en la conformación de esa planta).
- Fortalecimiento de las actividades de investigación y programa de posgrado.
- Consolidación de los esquemas de financiamiento del laboratorio.
- Fortalecimiento de las actividades de difusión y enlace con instituciones de educación superior.
- Fortalecimiento de las actividades de vinculación con el sector productivo de tecnologías de información.
- Avance en las instalaciones definitivas de **Cinvestav-Tamaulipas**.

Conclusiones

El Centro de Investigación y de Estudios Avanzados del IPN es la institución mexicana líder en materia de formación de recursos humanos a nivel posgrado. Su productividad científica representa una contribución importante al desarrollo científico de México. En el área de ingeniería, desde su fundación se ha cultivado un programa de Ingeniería Eléctrica, mismo que albergó durante 26 años el posgrado en computación. Como objeto de estudio y parte importante de las tecnologías de información, la computación ha sido desarrollada en el Departamento de Ingeniería Eléctrica en la Unidad Guadalajara y, desde el año 2006, en el Departamento de Computación. Algunas aplicaciones de la computación también son parte importante del quehacer científico que se desarrolla en departamentos académicos como Física, Matemáticas, Química, Fisiología, Física Aplicada, por citar sólo algunos ejemplos.

Si bien no existe un antecedente en el **Cinvestav** de tratar las tecnologías de información como una disciplina que contempla un conjunto de áreas, sí existen antecedentes de cada una de sus partes. En este número de la revista ***Cinvestav*** se reportan ejemplos de dichos antecedentes.

Crear un laboratorio dedicado al estudio y desarrollo de las tecnologías de información representa al **Cinvestav**, por un lado, un gran desafío y, por otro, una gran oportunidad para avanzar en su modelo de desarrollo descentralizado iniciado hace más de 20 años. Cuando se revisan las historias o reseñas sobre la creación de otras unidades del **Cinvestav** [13], resulta sorpresiva la visión de los precursores de dichas iniciativas y de los altos riesgos que enfrentaron para llevarlas a cabo. La circunstancia actual hace posible que una iniciativa como la del Laboratorio de Tecnologías de Información nazca fortalecida. Para la justificación del proyecto del laboratorio se han consultado diversas fuentes de información, disponibles fácilmente a través de las telecomunicaciones. Los estudios realizados por diversas organizaciones muestran que existe un gran interés en los temas relacionados con tecnologías de información. Se tiene una iniciativa conjunta apoyada directamente por un gobierno estatal y por los programas del gobierno federal.

La disponibilidad de investigadores en el área, si bien aún no es tan amplia y tan especializada como sucede en otros campos de la investigación científica, tampoco es ya tan escasa como se observaba hasta antes del año 2000. La disponibilidad de fuentes de financiamiento para un proyecto de esta naturaleza es diversa (aunque no tan amplia como se desearía). La oportunidad que tiene el **Cinvestav** para desarrollar esta nueva unidad es, en mi opinión, inmejorable. Dependerá de quienes participamos en ella, que las grandes expectativas generadas con la creación del Laboratorio de Tecnologías de Información se concreten y que los resultados para el desarrollo del estado de Tamaulipas y de México confirmen que las decisiones fueron correctas.

[Referencias]

[1] Association for Computing Machinery. *Computing Curricula 2005 – The Overview Report*. Abril 2006.

[2] Teléfonica, S. A. *La sociedad de la información en España*. http://www.telefonica.es/sociedaddelainformacion. Diciembre 2005.

[3] AMITI, CANIETI y FMD. *Vision 2020: Políticas públicas en material de tecnologías de información y comunicaciones para impulsar la competividad de México*. 2006.

[4] González Bañales Dora Luz. *Estudio exploratorio de los factores críticos de éxito de la industria Mexicana de software y relación a la orientación estratégica de negocio*. Universidad Politécnica de Valencia. Febrero 2006.

[5] Consejo Nacional de Ciencia y Tecnología. *Programa Especial de Ciencia y Tecnología 2001-2006*, tomo II. 2001.

[6] Secretaría de Economía. *Programa para el desarrollo de la industria del software (Prosoft)*. 2001.

[7] ANUIES. *Anuario Estadístico 2004. Población escolar de licenciatura y técnico superior en universidades e institutos tecnológicos*. 2006.

[8] ANUIES. *Anuario Estadístico 2004. Población escolar de posgrado 2006*.

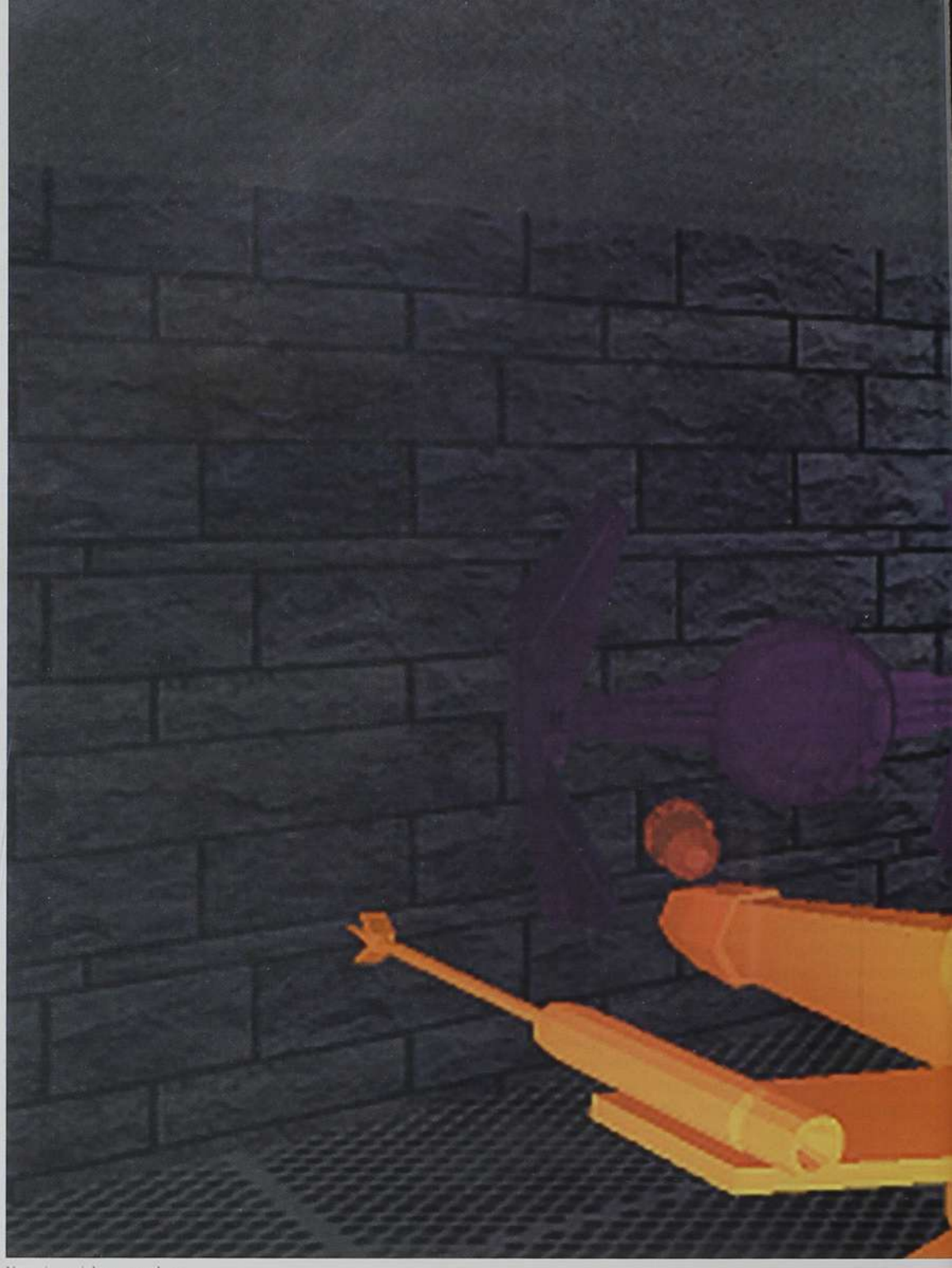
[9] http://www.software.net.mx/anuario/. Anuario Prosoft 2006.

[10] Gobierno del Estado de Tamaulipas. *Plan de Desarrollo Estatal de Desarrollo 2005-2010*. 2005.

[11] Secretaría de Economía. *Reporte de Potencialidades de las Entidades Federativas para Desarrollar Núcleos de Economía Digital*. Diciembre 2002.

[12] Gobierno del Estado de Tamaulipas y Cluster Tamaulipas de Tecnologías de Información A. C. *Reporte preliminar del Estudio de Competitividad de la Industria de Tecnologías de Información de Tamaulipas*. Abril 2006.

[13] Ibarrolla, M., P. Cabrera, R. Asomoza, E. Frixione, A. García, M.A. Pérez Angón y S. Quintanilla. *El Cinvestav: Trayectoria de sus departamentos, secciones y unidades, 1961-2001*. Centro de Investigación y de Estudios Avanzados del IPN. México, D.F. 2002.

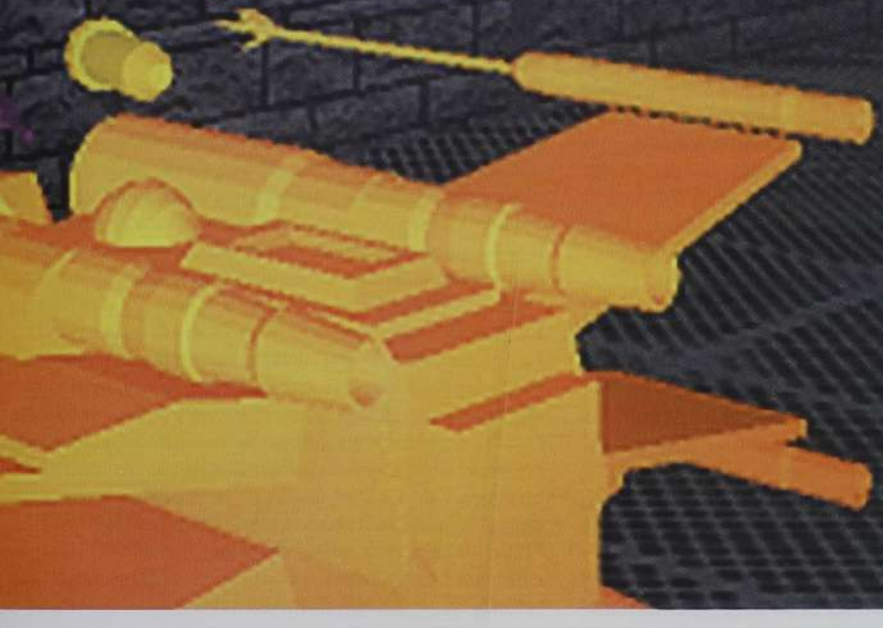


Naves imperiales en combate.

El Grupo de Ciencias de la Computación en el Cinvestav-Guadalajara

LA UNIDAD GUADALAJARA, IGUAL QUE LAS OTRAS SEDES DEL CINVESTAV, FUE CREADA PARA APOYAR LAS PRINCIPALES ACTIVIDADES ECONÓMICAS DE LA ENTIDAD EN QUE RADICA. EN JALISCO, LA INDUSTRIA DE TECNOLOGÍAS DE LA INFORMACIÓN HA GANADO TERRENO, Y ES EN ESE DINÁMICO AMBIENTE DONDE SE ENMARCA EL DESARROLLO DEL GRUPO DE CIENCIAS DE LA COMPUTACIÓN.

Félix Francisco Ramos Corchado



FÉLIX FRANCISCO RAMOS CORCHADO Se doctoró en 1997 en la Universidad de Tecnología de Compiègne (Francia); en el **Cinvestav** se tituló como maestro en Ciencias y, en el Centro Nacional de Artes y Oficios de París, obtuvo el Diploma de Estudios Avanzados; es ingeniero por la Universidad Autónoma Metropolitana. Desde 1998 trabaja como investigador en el grupo de Ingeniería Eléctrica del **Cinvestav** en Guadalajara. En 1999 creó un simposio y una escuela internacional en Sistemas Distribuidos Avanzados (ISSADS). Dicho evento cuenta con el reconocimiento del *Insititute of Electrical and Electronic Engineers* (IEEE) y sus memorias son publicadas en Springer Verlag. Sus áreas de interés abarcan los sistemas distribuidos e inteligentes, la realidad virtual y sistemas autoorganizables.
framos@gdl.cinvestav.mx

Desde su creación, el Grupo de Ciencias de la Computación participa en el desarrollo de la industria de tecnologías de la información, ya sea mediante la inserción directa de sus egresados o por la vía de cursos de actualización, desarrollo de habilidades o de sistemas, según lo requiera dicha industria.

Breve historia del grupo

La Unidad Guadalajara del **Cinvestav** inició sus actividades en el año de 1988 con el Centro de Tecnología de Semiconductores (CTS), el cual es una casa de diseño en sistemas electrónicos y de *software*. En 1995, aunado a esa actividad, se iniciaron las actividades académicas del Departamento de Ingeniería Eléctrica y Ciencias de la Computación (DIECC).

El Grupo de Ciencias de la Computación se formó en 1998 y fue el cuarto de un total de cinco grupos de investigación en la Unidad Guadalajara. En orden cronológico, estos grupos son: Control Automático, Telecomunicaciones, Sistemas de Potencia, Ciencias de la Computación y Diseño Electrónico. Desde su inicio, el programa de maestría ha estado inscrito en el Programa Nacional de Posgrado (PNP) del Consejo Nacional de Ciencia y Tecnología (Conacyt). En 1998 se instauró el programa doctoral, el cual también desde su inicio está inscrito en el PNP del Conacyt. El grupo principió con dos profesores permanentes, que establecieron el programa inicial de la especialidad, y varios profesores invitados. Actualmente tiene cinco profesores permanentes. La población dentro de los dos programas es un promedio de 25 candidatos a maestría en Ciencias por año y cuenta con un permanente de alrededor de 15 candidatos a doctorado. Este número está limitado por el número de miembros que tiene el grupo y por los lineamientos que establece el Conacyt.

Programas y formas de ingreso

Los candidatos a maestría son captados mediante promoción que realiza anualmente la Unidad Guadalajara en las ferias de ciencia en el país y visitas explícitas a seleccionados centros de educación superior. Esto quiere decir que el ingreso al programa de maestría es anual. De acuerdo con las estadísticas de nuestra unidad, más de 40% de las solicitudes de ingreso son para la maestría con el Grupo de Ciencias de la Computación. Los candidatos inscritos en el programa de maestría pasan por un cuidadoso mecanismo de selección que dura alrededor de dos meses y medio e inicia con un examen de selección previo, seguido de un curso propedéutico, y finaliza con un examen de conocimiento y entrevistas personales. En porcentaje, menos de 10% de los aspirantes son admitidos al programa de maestría. La eficiencia terminal del Grupo de Ciencias de la Computación es superior a 75%.

El programa de doctorado, a diferencia del de maestría, está abierto durante todo el año. Existen dos modalidades de ingreso: la primera es llamada *doctorado directo* y la segunda, *doctorado*. En la primera modalidad, los candidatos ingresan con un diploma de ingeniería o un diploma universitario de conocimientos afines y siguen el proceso de ingreso a la maestría. Una vez inscritos al programa de doctorado directo, tienen cuatro años para cursar los créditos equivalentes a los de maestría y terminar su investigación doctoral. En la segunda modalidad, el candidato ya posee una maestría afín a la especialidad y sólo realiza un examen de admisión, que sirve para determinar si es apto para ingresar al programa y qué formación se le recomienda seguir para fortalecer su formación integral.

Relación del grupo en la entidad

La Unidad Guadalajara, de la misma manera que otras Unidades del **Cinvestav**, fue generada para apoyar alguna(s) de las principales actividades económicas de la entidad en que radica. Jalisco, además de ser uno de los principales productores nacionales de lácteos y cárnicos, ha promovido las tecnologías de la información. La importancia de la industria electrónica y de *software*, tanto en número como en el reconocimiento de las empresas internacionales establecidas en la entidad, ha valido a la región el nombre de *Silicone Valley* mexicano desde hace ya más de un sexenio. Es en ese ambiente donde podemos enmarcar el desarrollo del grupo y sus relaciones en la entidad, a saber: con la industria, el gobierno y las instituciones de educación superior.

En cuanto a su relación con la industria local, hay que señalar que, desde su creación, el grupo participa

La sede del Grupo de Ciencias de la Computación en Guadalajara.

en el desarrollo de la industria de tecnologías de la información, ya sea mediante la inserción directa de sus egresados o por la vía de cursos de actualización y desarrollo de habilidades y de sistemas, orientados a las áreas específicas de esta industria.

Existen dos modalidades del desarrollo de sistemas: en la primera, el grupo realiza y se hace responsable de proyectos que se encuentran completamente a su cargo; en la segunda, el grupo establece un convenio de colaboración entre alguno de los investigadores y alguna compañía de prestigio, se firman convenios de confidencialidad y se involucra un estudiante de maestría o doctorado para resolver problemas específicos que requiera este tipo de recurso humano altamente calificado.

La relación con el gobierno es muy estrecha. Consiste de convenios que dan al **Cinvestav** la responsabilidad de generar programas de capacitación para la industria, mientras que el financiamiento de todo el desarrollo del programa corre a cargo del gobierno. El grupo ha participado en tres de estos convenios: uno, llamado Programa Avanzado de Diseño de Sistemas (PADS), está orientado a la capacitación en diseño de sistemas electrónicos; el segundo es el Programa Avanzado para el Fortalecimiento de las Tecnologías de la Información (PAFTI), y el tercero se dedica a la formación de recursos en sistemas embebidos. El monto de estos proyectos es de alrededor de 2.5 millones de pesos.

La relación con otras instituciones educativas, que se ha ido generando a lo largo del tiempo, es un punto muy importante para el grupo. En el caso de las instituciones de educación superior nacional, son principalmente nuestros candidatos a maestría y doctorado los que se insertan o mantienen contacto con ellas. El grupo imparte, por invitación, conferencias magisteriales en eventos organizados por esas instituciones y lleva a cabo cursos de actualización para sus profesores; además, se están iniciando cooperaciones en proyectos conjuntos. Con laboratorios y universidades de otros países se han generado grupos de trabajo que permiten complementar trabajos de investigación; asimismo, se elaboran proyectos conjuntos que involucran a los estudiantes por medio de sus temas de tesis de maestría o doctorado. Las colaboraciones que se tienen actualmente incluyen universidades de Francia, Inglaterra, Alemania y Estados Unidos, principalmente.

La currícula en Ciencias de la Computación

Desde su inicio, el Grupo de Ciencias de la Computación estableció claramente que los sistemas distribuidos sería el área de su investigación, básicamente por el interés y la importancia que ocupa en computación, así como por el vínculo que tiene con las demás áreas del conocimiento. La currícula para la maestría en Ciencias de la Computación está compuesta de alrededor de veinte cursos. El candidato a maestría debe cubrir cinco cursos obligatorios y los restantes están orientados al tema que elige para su investigación. Los cursos obligatorios son: Teoría de lenguajes y autómatas, Lógica matemática, Teoría de grafos, Ingeniería de *software* y Algoritmia y complejidad. Entre los cursos optativos están: Redes de Petri, Sistemas distribuidos, Sistemas multiagentes, Sistemas de eventos discretos, Probabilidad y estadística, Inteligencia artificial, Redes de computadoras (I y II), Aprendizaje, Meta aprendizaje,

Métodos formales para ciencias de la computación, Temas selectos de computación, Matemáticas, etcétera. La currícula del candidato a doctorado está constituida de por lo menos tres cursos, que complementan su formación.

Infraestructura

El grupo dispone de un espacio de aproximadamente 400 m^2. De esta área, 50% está destinado a las instalaciones para los estudiantes y el resto corresponde a los siguientes laboratorios: Sistemas distribuidos, Redes, Realidad virtual y Sistemas embebidos (laboratorio que cuenta con una inversión de 2.5 millones de pesos).

Planeación a futuro

Siempre en la dirección de los sistemas distribuidos, el grupo planea contar con diez integrantes. Se espera de ellos que apoyen la formación de los recursos humanos que genera el grupo y emprendan, con metodologías apropiadas, proyectos multidisciplinarios que contribuyan al desarrollo del área en nuestra región y país. A continuación se describe el perfil de los futuros integrantes del grupo y cuál deberá ser su aportación al grupo.

- *Doctor en Ingeniería de software*. Este recurso permitirá al grupo apoyar la formación de nuestros estudiantes y proporcionará una metodología apropiada para proyectos multidisciplinarios.
- *Doctor en Computación paralela, lenguajes y compiladores*. Este recurso permitirá al grupo desarrollar actividades de sistemas distribuidos; por ejemplo, cómputo masivo, necesario para efectuar animación 3D, enlace computacional con otras instituciones nacionales y fortalecimiento de la formación de los egresados en temas tan importantes como lo son los lenguajes.
- *Doctor en Graficación*. Este recurso permitirá complementar la formación de los recursos humanos y, al grupo, generar motores gráficos para fortalecer el equipo de SMA y RV y demás con otros equipos de la Unidad, y así poder participar en proyectos multidisciplinarios.
- *Doctor en Sistemas móviles*. Este recurso fortalecerá la formación de recursos en proyectos de SMA-RV y permitirá realizar trabajos con tecnologías para aplicaciones móviles, como lo son los sistemas embebidos.
- *Doctor en Sistemas complejos*. Este recurso colaborará en proyectos de sistemas distribuidos, sistemas multiagentes, sistemas móviles y sistemas de vida artificial. Además de completar las competencias para realizar proyectos con más complejos, deberá ser vínculo con otros grupos de nuestra Unidad y de otros centros del **Cinvestav** o fuera de él.

Líneas de investigación

Las líneas de investigación se han enriquecido conforme el grupo ha crecido y se han establecido convenios de cooperación con otros laboratorios de investigación nacionales e internacionales. A continuación se describen las áreas de investigación de cada uno de los integrantes del grupo.

FÉLIX RAMOS. Sus líneas de investigación son sistemas multiagentes, *middleware*, realidad virtual, vida artificial y sistemas autoorganizables.

En el año 2000, el Doctor inició un proyecto en el cual involucró a investigadores de otros laboratorios, como son los pertenecientes al INPG, la Universidad de Valenciennes, la Universidad Tecnológica de Compiègne y el Instituto de Investigaciones en Informática de Toulouse de Francia y la Universidad de Rostock de Alemania. Este proyecto resume las líneas de trabajo del investigador. Se enfoca en el desarrollo de una plataforma orientada a usuarios finales para que éstos a su vez puedan elaborar aplicaciones de realidad virtual mediante una descripción en un lenguaje de tipo natural. El funcionamiento básico del sistema se muestra en la figura 1.

El nombre genérico del proyecto es *Generic Distributed Architecture for 3D Applications* (GeDA • 3D). Involucra diferentes áreas, que van desde lenguajes hasta motores

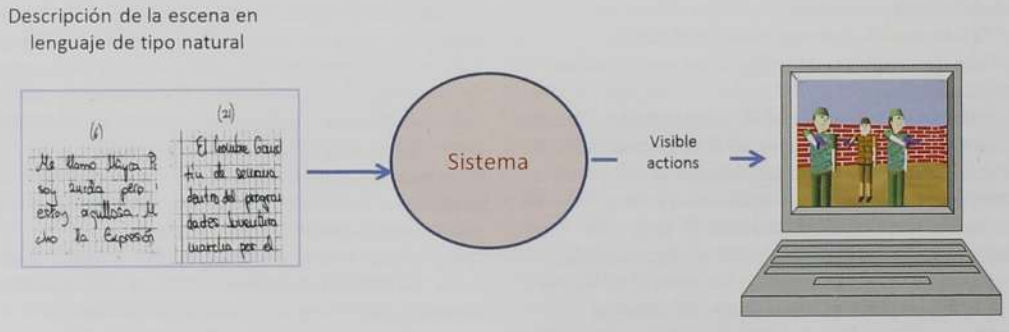


Figura 1. Funcionamiento básico de GeDA • 3D.

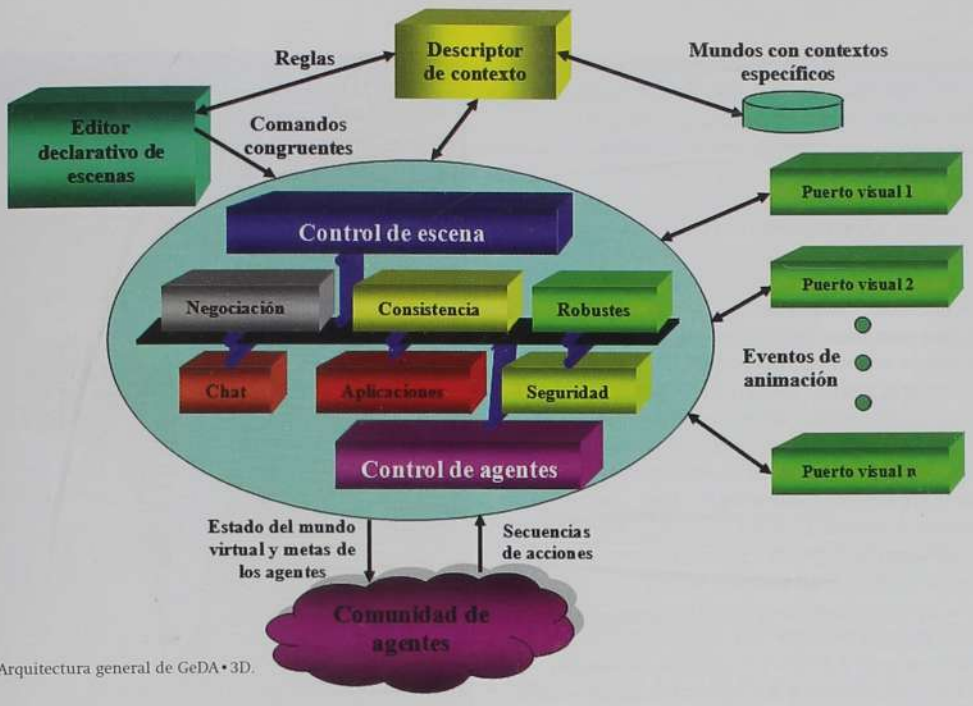


Figura 2. Arquitectura general de GeDA•3D.

de *rendering* del lado de ingenierías y varias áreas de tipo social y psicológico. La figura 2 muestra la arquitectura de la plataforma, la cual está constituida por un conjunto de componentes distribuidos y conectados mediante una red. El funcionamiento de esta arquitectura es descrito brevemente a continuación.

El usuario proporciona al sistema una descripción de un sistema (escena) en un lenguaje de tipo natural al módulo *editor declarativo*. La descripción debe contener los actores de la escena, la forma en que constituido el escenario y una descripción del tipo de contexto en que se realiza la escena. Este módulo se encarga de verificar la semántica, las restricciones geométricas y la congruencia de la descripción de entrada. Si el análisis resulta positivo, entonces se pasa una cadena formateada en un lenguaje matemático al núcleo de GeDA•3D [1], el cual se encarga de: 1) activar los agentes necesarios a cada actor de la escena; 2) indicarles a cada uno las metas que tienen que satisfacer, así como las restricciones temporales para que éstas ocurran, y 3) indicar al puerto(s) visual la descripción del escenario. Los agentes de GeDA•3D toman las metas que les fueron asignadas e inician los procesos (cognitivos y temporales) necesarios para alcanzarlas, ya que la descripción indica las metas mas no la forma en que deberán ser alcanzadas. Además, dado que el ambiente está regido por un contexto que especifica las leyes que gobiernan un mundo, los agentes tienen restricciones en las decisiones que tomen para alcanzar sus metas. La arquitectura de agente propuesta en este trabajo considera emociones con el objetivo de obtener mayor realismo en aplicaciones de tipo humano. Las emociones [2] modifican el comportamiento de un agente. No es lo mismo abrir una puerta cuando el agente está contento que cuando está triste, tampoco lo es su forma de caminar ni de moverse. Una vez que los agentes fueron generados, configurados con las personalidades indicadas en la descripción, son asignados a un avatar, que representará gráficamente cada una de las decisiones que tomen estos agentes y es representada por medio del *puerto visual*, el cual, como se indica en la figura 2, puede ser único o múltiple.

La utilidad de una plataforma es genérica, ya que permite generar diferentes tipos de aplicaciones, por ejemplo: tipo cinema, donde se define un *script* y se solicita a la plataforma realizarlo; tipo simulación de situaciones de desastres naturales, u otros, como diseño de planes de evacuación en situaciones peligrosas,

Actualmente, el Doctor Félix Ramos participa en un proyecto internacional, llamado *Generic Distributed Architecture for 3D Applications*, que comprende la creación de una plataforma que involucra diferentes áreas, desde lenguajes hasta motores de *rendering* del lado de ingenierías y varias áreas de tipo social y psicológico.

planeación urbana, entrenamiento o enseñanza, diseño distribuido, etcétera. Estos variados tipos de aplicaciones complejas son posibles, principalmente, porque la plataforma puede estar distribuida de manera geográfica, lo cual permite escalar a GeDA•3D.

Actualmente, en el proyecto se realizan investigaciones sobre editores declarativos, formas de extender la plataforma a ambientes inalámbricos, animación de esqueletos, protocolos de juegos, emociones, ontologías aplicadas a la generación de contextos para mundos virtuales. El trabajo se realiza con equipos de investigación de Francia y Alemania.

Entre las aplicaciones desarrolladas se encuentra un juego de estrategia básico, en el cual dos ejércitos contrarios inician una lucha por el poder consiguiendo las riquezas de un territorio, al tiempo que intentan eliminar al rey del imperio contrario. Otro ejemplo es de unas naves que combaten en un laberinto y que, además de localizar a su enemigo, tienen que resolver restricciones geométricas, es decir, calcular los espacios por donde pueden pasar; la aplicación siguiente sobre la plataforma maneja la influencia de las emociones en el comportamiento de agentes. Finalmente, tenemos algunos resultados sobre la generación de un escenario y la evolución de una escena realizada por más de un avatar [3]; ambos, el escenario y la escena, son descritos en un lenguaje declarativo.

Las investigaciones que actualmente se realizan están enfocadas en la animación de diferentes esqueletos en tiempo real, en la generación de manejadores para dispositivos "hápticos", que permitan la interacción con los mundos reales y manejo de protocolos para acceder a aplicaciones de tiempo real distribuidas, así como en la creación de manejadores que incluyan en las aplicaciones otros medios, como son audio y video.

ERNESTO LÓPEZ. El trabajo del investigador trata de la especificación formal de sistemas distribuidos que pueden ser modelados con técnicas del tipo de *eventos discretos*. Más específicamente, los temas de este estudio se pueden desglosar en los siguientes tres puntos:

- *Especificación formal de sistemas de eventos discretos complejos.* En este tema se utilizan las redes de Petri como formalismo de base para modelar el comportamiento deseado de los sistemas a implementar. Se definió un formalismo multinivel, llamado nLNS, que sigue el enfoque de redes dentro de redes, mediante el cual se obtienen modelos modulares y jerárquicos de sistemas complejos que incluyen entidades móviles; con este formalismo se han podido abordar problemas de sistemas de manufactura, comunidades de robots móviles, de comercio electrónico, de simulación de tráfico urbano y de coordinación de flujo de trabajo [4].

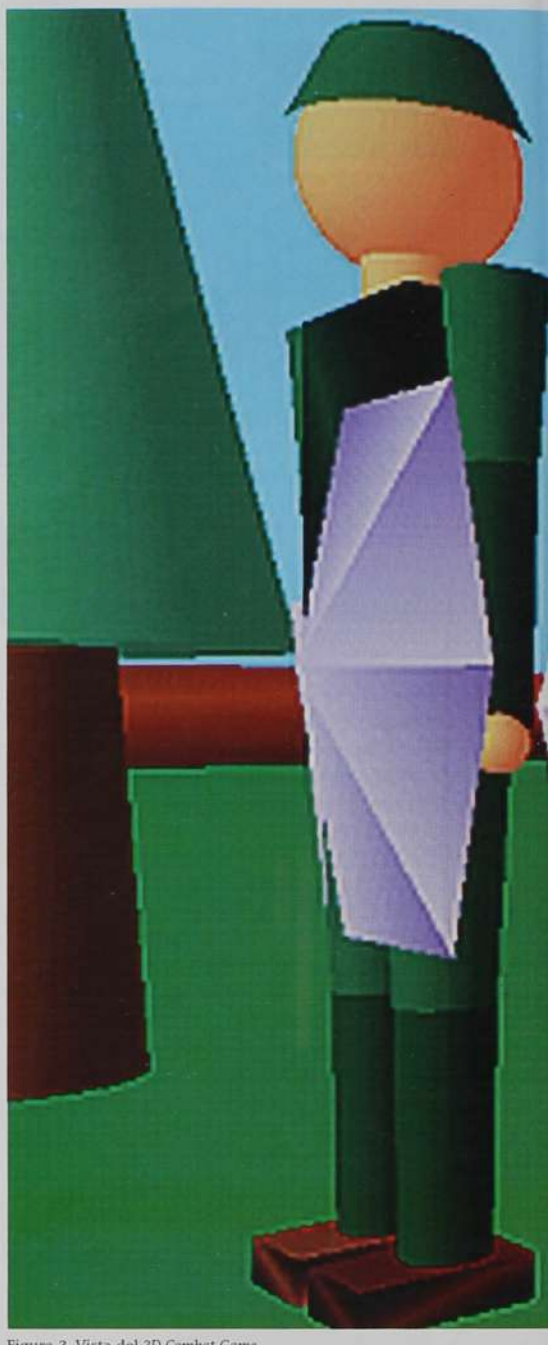


Figura 3. Vista del *3D Combat Game*.

El Doctor Ernesto López trabaja en la especificación formal de sistemas de eventos discretos complejos, en metodologías de desarrollo de sistemas multiagentes basado en agentes móviles y en los problemas de diagnóstico de faltas y la reconfiguración de los controladores o coordinadores.

- *Síntesis de* software *basado en agentes móviles*. Se ha trabajado en la obtención de metodologías de desarrollo de sistemas multiagentes que incluyen agentes móviles. A partir de especificaciones expresadas en nLNS se obtiene de manera sistemática la codificación en Java de agentes reactivos y código emigrante utilizando el *middleware* JADE. Actualmente se ha desarrollado una herramienta que permite editar modelos en nLNS, simularlos y generar automáticamente el *software* [5].
- *Coordinación tolerante a faltas*. Aquí se abordan los problemas de diagnóstico de faltas y la reconfiguración de los controladores o coordinadores. Sobre el diagnóstico se ha caracterizado estructuralmente la diagnosticabilidad y se han propuesto dos esquemas diagnosticadores; asimismo se trabaja en diagnóstico distribuido confiable. Cuando una falta es detectada y localizada, el sistema puede recuperar su funcionamiento a través de la reconfiguración del controlador. Se ha propuesto una técnica de reconfiguración basada en reescritura de modelos en redes de Petri [6].

MARIO SILLER. Las siguientes líneas ilustran el trabajo de este investigador.

La transmisión de servicios de multimedia (voz, video y datos) sobre redes de conmutación de paquetes se ha incrementado considerablemente en los últimos años. Esto se debe, entre otras cosas, al incremento en la capacidad de dichas redes, desarrollo de *software* más avanzado, el Internet y la proliferación de dispositivos disponibles a los usuarios (PDA, celulares, etcétera). El incremento de ancho de banda deriva del uso de nuevas tecnologías, tanto en la parte de acceso como de transporte de la red (DSL, GSM y otros). Sin embargo, nuevas formas de acceso y servicio han llevado al desarrollo de nuevas aplicaciones [7]. Esto significa que a pesar del incremento de ancho de banda, estas últimas pueden estar compartiendo dicha capacidad con las aplicaciones ya existentes. De ello la importancia y necesidad de los mecanismos de calidad de servicio y la codificación/compresión de los servicios de multimedia.

Existen mecanismos de calidad de servicio tanto para redes convencionales como activas. En una red convencional, la conmutación de paquetes se lleva a cabo a través del acceso de los campos de control, contenidos en los distintos encabezados que realiza el nodo receptor, donde se avanza de acuerdo con un protocolo determinado. En una red activa, en cambio, el nodo retransmisor va más allá de los encabezados accediendo al campo de datos de los paquetes y procesándolo con base en su configuración. El concepto de redes activas surge de discusiones realizadas por la comunidad investigadora perteneciente a DARPA sobre

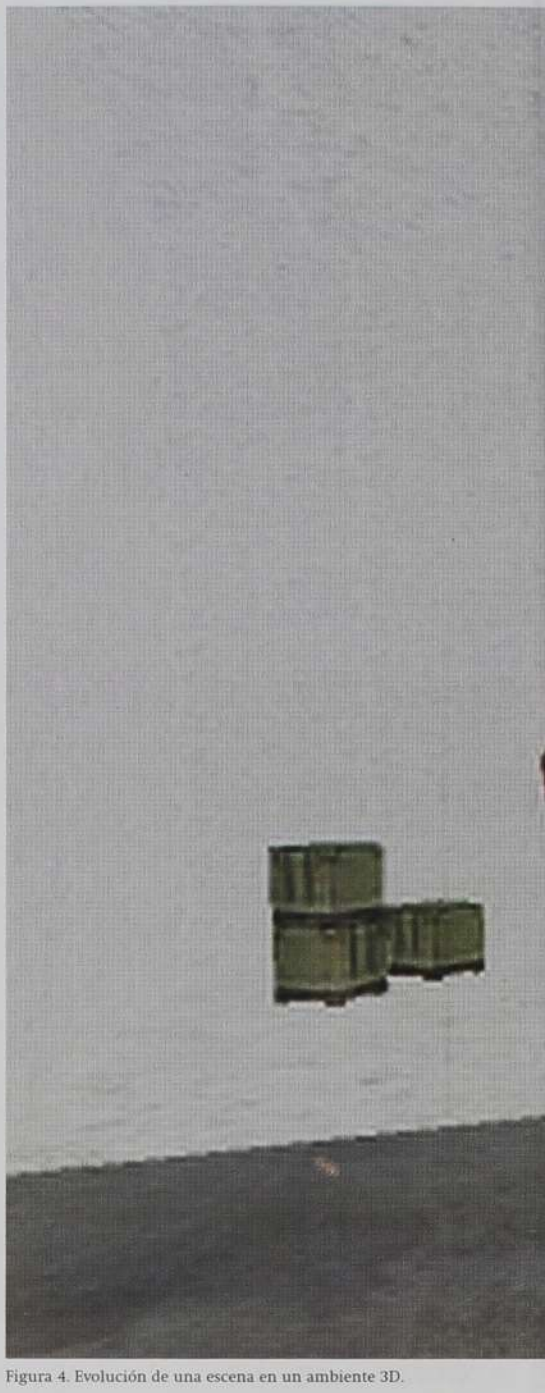


Figura 4. Evolución de una escena en un ambiente 3D.

Los mecanismos de calidad de servicio, tanto para redes convencionales como para las activas, y la codificación/comprensión de los servicios de multimedia es el tema de investigación del Doctor Mario Siller.

Figura 5. Influencia de las emociones en el comportamiento de las entidades.

QoS Research Network

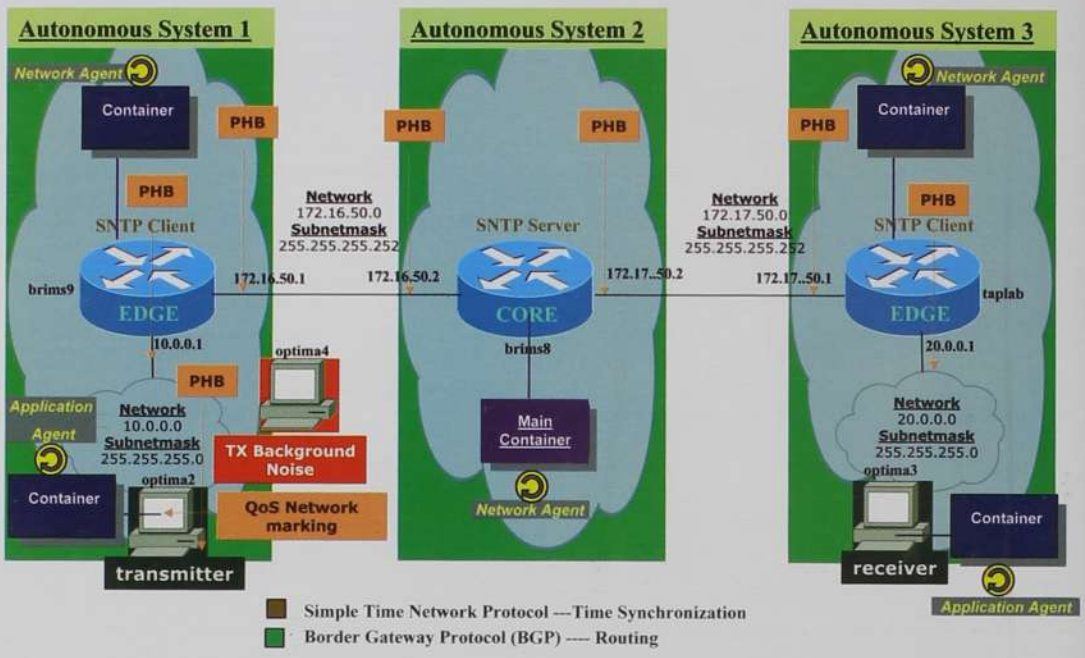


Figura 6. Cama de prueba.

el futuro de los sistemas de red en 1994 y 1995. En [8] una red activa se define como "una red que permite a los *routers* intermedios realizar operaciones de cómputo hasta la capa de aplicación".

En el caso de las redes convencionales, algunos mecanismos disponibles son: servicios diferenciados, definidos por la IETF en sus RFCs 2474, 2475, 2597 y 2598; servicios integrados, definidos por la IETF en su RFCs 1633, 2210, 2211 y 2212; multiprotocolo de conmutación por etiquetas (MPLS), desarrollado originalmente por CISCO y estandarizado por la IETF en sus RFCs 3031, 3032, 3036 y 3037; ingeniería de tráfico, RFC 2702; y ruteo basado en restricciones, RFC 2386. En cuanto a redes activas, algunos mecanismos disponibles incluyen control de errores a nivel red, recodificación, filtrado de tráfico (tirado inteligente de paquetes y transcodificación), dispersión de tráfico y retransmisiones.

La investigación en redes activas abarca las áreas de arquitectura, seguridad, mecanismos de calidad de servicio y aplicaciones. En el caso del Dr. Siller, su investigación de mecanismos de calidad de servicio se enfoca,

principalmente, a tres tipos de ellos: recodificación, filtrado y dispersión de tráfico. En este sentido he desarrollado algoritmos de filtrado inteligente de paquetes, que consisten en la eliminación de paquetes redundantes de la red de flujos de video codificados en MPEG y H263. La redundancia se determina por la tasa de pérdida de paquetes de tipo marco I (*I frame*), de tal forma que cuando se presenta dicha condición, los paquetes de tipo B y P relacionados con dicho marco son eliminados en forma activa. En cuanto a la investigación de administración de calidad de servicio, se ha desarrollado una plataforma de gestión y un marco de referencia basados en el uso de métricas de desempeño de red, requerimientos del usuario final y retroalimentación de calidad de experiencia en tiempo real. Este trabajo es presentado en [9].

Las redes de telecomunicaciones han experimentado grandes cambios en los últimos años, visibles tanto en la tecnología como en el uso de paradigmas nuevos. El proceso que ha ido ocurriendo puede resumirse en una sola palabra: *convergencia*. Este nuevo escenario de red y su ubicuidad, desde la parte de acceso hasta el transporte, nos permite considerar a las redes activas y los mecanismos de calidad de servicio fundamentales para el desarrollo de las telecomunicaciones en el siglo XXI. Les permitirá tener, por un lado, la capacidad de programar o personalizar la red de acuerdo con las aplicaciones, y por otro, la flexibilidad y rapidez de configuración de nuevos servicios.

El trabajo experimental se realiza a través de simulaciones y *testbeds*, tal y como se muestra en la figura 7. En resumen, las líneas de investigación cultivadas son: mecanismos de calidad de servicio en redes convencionales y activas; medición y mapeo de la calidad de experiencia a servicio en redes de telecomunicaciones; transmisión y codificación de servicios de multimedia y redes activas.

RICARDO VILALTA. Su trabajo se enfoca en el campo del reconocimiento de patrones, el área de estudio que se divide normalmente en dos partes: la extracción de señales y la clasificación de patrones. La primera parte toma como entrada una señal (*e.g.*, imagen, sonido, voz, etcétera) e intenta extraer atributos relevantes de tal señal. Por ejemplo, el reconocimiento de objetos luminosos de imágenes obtenidas a través de telescopios modernos requiere un procesamiento de imágenes que permita identificar aquellos objetos que sobresalen por su brillantez. Una vez extraídos esos atributos de la imagen, el segundo paso consiste en tratar de agrupar o clasificar los objetos identificados entre una de varias categorías. En el ejemplo aludido, un objeto luminoso podría ser clasificado como estrella, planeta, galaxia, etcétera.

Uno de los objetivos en el reconocimiento de patrones está en construir sistemas computacionales que aprendan a predecir la categoría a la que pertenecen las entidades de análisis. Existe un número extenso de aplicaciones en el área, como lo son el otorgamiento de crédito a instituciones financieras, la predicción del desdoblamiento de proteínas en tres dimensiones, el reconocimiento de caracteres, la predicción del desempeño de unidades de cómputo, entre otras.

El trabajo del investigador se centra en el desarrollo de nuevos algoritmos de clasificación que se adapten a las características de los datos. A diferencia de otras líneas de investigación, en ésta se explora la forma en que se relacionan los datos con el mecanismo de clasificación. La idea esencial es que la distribución de los datos debe dictar el mecanismo apropiado para conseguir predicciones de alta precisión. Si los datos cambian, el mecanismo de clasificación debe asimismo cambiar. Esta línea de investigación, conocida como metaaprendizaje, en los últimos años ha mostrado grandes avances.

Estas investigaciones han llevado a su autor al terreno de la física. En conjunto con el Dr. Tomasz Stepinski del Instituto Lunar y Planetario en Houston (Texas) trabaja en la creación de una herramienta para el análisis de la topografía de Marte. El proyecto se enfoca en la caracterización de sus distintas formaciones geológicas. Actualmente, el estudio de la superficie de Marte se realiza principalmente a través del análisis manual de imágenes obtenidas por satélites que giran a su alrededor. El proceso es laborioso y no es posible abarcar mucho de la superficie del planeta sin herramientas que permitan automatizar el análisis de datos.

El objetivo en este proyecto es conseguir la generación automática de mapas digitales de Marte que

El Doctor Ricardo Vilalta participa en un llamativo proyecto en conjunto con el Instituto Lunar y Planetario de Houston, que trata de conseguir la generación automática de mapas digitales de Marte para identificar las distintas formaciones geológicas a lo ancho del planeta.

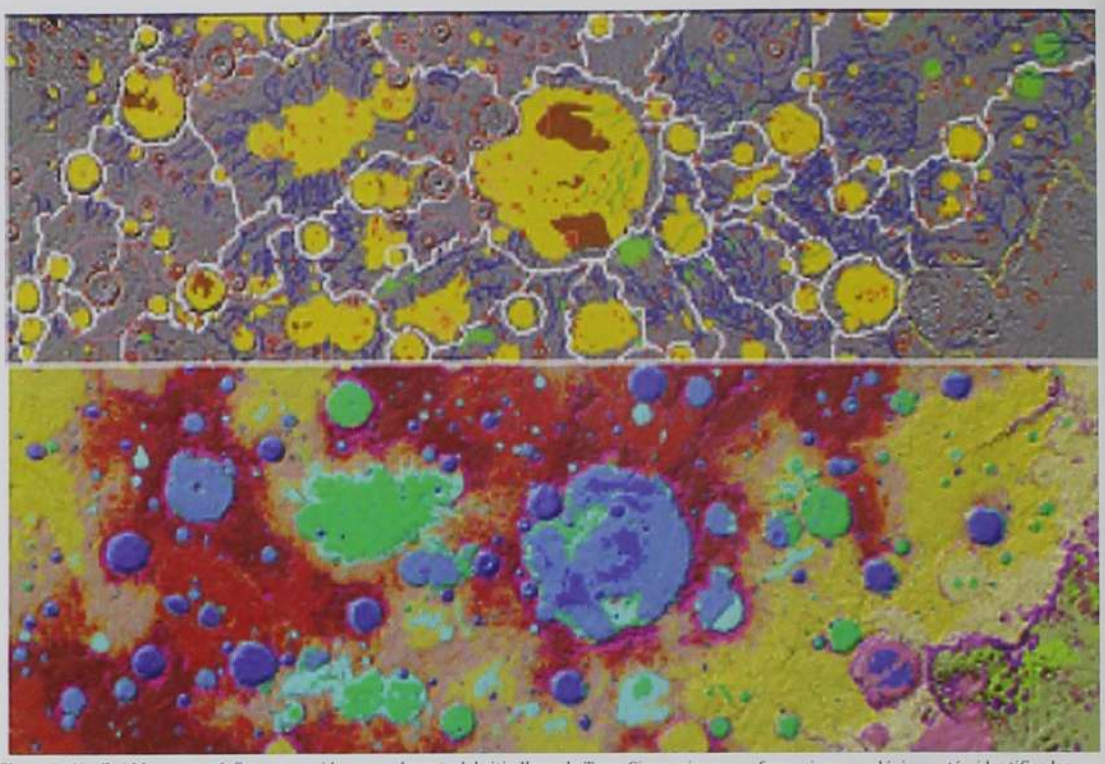


Figura 7. (Arriba) Mapa geomórfico construido manualmente del sitio llamado Terra Cimmeria; nueve formaciones geológicas están identificadas, con una región extensa sin ninguna designación. (Abajo) Mapa obtenido con técnicas de agrupación de datos usando atributos topográficos, que dio como resultado 19 categorías.

identifiquen las distintas formaciones geológicas de cada sitio en el planeta (cráteres, valles, canales, etcétera). La figura 7 muestra un ejemplo de lo que varias herramientas provenientes del reconocimiento de patrones son capaces de hacer. En la parte alta se aprecia un mapa generado manualmente por expertos; en la baja, un mapa generado automáticamente por un algoritmo de reconocimiento de patrones. Este mapa es mucho más preciso en la identificación de formaciones geológicas y cuenta con la gran ventaja de ser extremadamente rápido en el procesamiento de datos.

RAÚL ERNESTO GONZÁLEZ TORRES. Desde hace cinco años, su principal área de investigación está en el desarrollo y la implementación de métodos para verificar formalmente, de preferencia de manera automática, modelos de sistemas de procesos, circuitos secuenciales y protocolos de comunicación, empleando herramientas de verificación que el investigador y su equipo han ido produciendo.

Las especificaciones o propiedades a verificar en el modelo de un sistema dado, típicamente se traducen de su formulación inicial en lenguaje natural a un lenguaje de lógica temporal. Con el objeto de hacer más ágil (semiautomático) y objetivo el proceso de traducción, se han detectado patrones que describen ciertos tipos de especificaciones, que generalmente se desea se cumplan, o que no se cumplan, en una determinada clase de sistemas.

Entre los métodos de verificación formal, el conocido como Comprobación de Modelos (*Model Checking*) es actualmente el que atrae mayor interés, por poseer las características de estar matemáticamente bien fundamentado y por ser automatizable en casi todas sus etapas (ver figura 8).

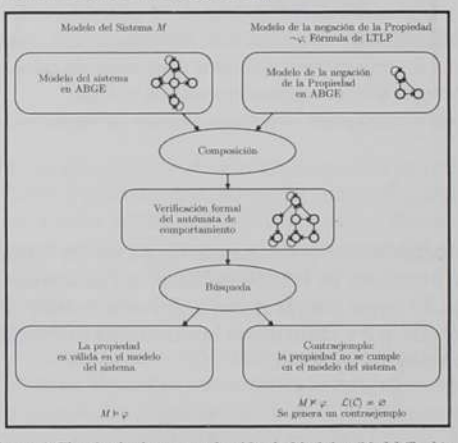


Figura 8. El método de comprobación de Modelos *(Model Checking)*.

Descubrir e implementar diversas técnicas y heurísticas para combatir el llamado problema de explosión del espacio de estados, que se presenta en la verificación por comprobación de modelos de sistemas de tamaño real, es la línea de investigación que actualmente trabaja el Doctor Raúl Ernesto González Torres.

Pero el obstáculo principal para efectuar la verificación por Comprobación de Modelos de sistemas de "tamaño real" es el llamado *problema de explosión del espacio de estados*: los modelos a verificar alcanzan un tamaño exponencialmente mayor que el número de variables empleadas para describir el comportamiento de un sistema dado. Como consecuencia, hasta ahora este método de verificación, por lo general, sólo es aplicable de manera efectiva a sistemas con un número relativamente pequeño de variables (y estados). El objetivo de los investigadores consiste, entonces, en descubrir e implementar diversas técnicas y heurísticas que permitan combatir este problema, y así poder aspirar a que sus herramientas de verificación formal adquieran amplia aceptación en el mundo del diseño y fabricación de los productos y servicios que emplean las personas. Algunas de las técnicas para combatir el problema de explosión de estados descubiertas más recientemente son: el razonamiento composicional (o modularidad), la reducción por orden parcial y la comprobación simbólica (con o sin BDD's). El equipo está estudiando y experimentando estas técnicas con herramientas propias de verificación, tanto de manera aislada como conjunta, tomando como casos de estudio algunas *benchmarks* establecidas (como Texas'97) y algunos sistemas de procesos usados con frecuencia como prototipos en la literatura científica.

Proyectos en los que actualmente trabaja el doctor están relacionados con estas líneas de investigación:

- Aplicación de técnicas de reducción del espacio de estados en la verificación de circuitos digitales.
- Generación semiautomática de especificaciones en lógica temporal mediante el uso de patrones.
- Verificación composicional simbólica de circuitos secuenciales usando técnicas de aprendizaje para la generación automática del entorno.
- Aplicación de la interpolación de Craig en la comprobación de modelos.
- Comprobación de modelos simbólica usando algoritmos SAT en lugar de BDD's.

Paralelamente trabaja en la síntesis de controladores supervisores y controladores procedurales, por constituir otro campo donde la lógica temporal y los métodos empleados en la verificación formal pueden tener un impacto significativo. Participa en la creación de un círculo virtuoso síntesis-verificación-síntesis, tan automatizado como sea posible. Esto implica la necesidad de encontrar marcos de modelado igualmente adecuados para la síntesis como la verificación, así como la necesidad de poner especial atención a los contraejemplos que suelen arrojar los algoritmos de verificación; requieren ser analizados cuidadosamente y usarse como guía para descubrir la manera en que debe ser modificado el lenguaje generado por el modelo del sistema controlado.

Proyectos en los que está involucrado y que se relacionan con esta línea de investigación son los siguientes:

- Síntesis de controladores supervisores mediante la verificación formal usando cálculo μ.
- Síntesis modular de controladores supervisores para sistemas de procesos.
- Uso de técnicas de abstracción en la síntesis de controladores lógicos para sistemas industriales.
- Verificación de propiedades de seguridad y vivacidad en sistemas de eventos discretos controlados.

[Referencias]

[1] Piza, Iván H., Fabiel Zúñiga y Félix F. Ramos. A Platform to Design and Run Dynamic Virtual Environments, *IEEE Cyberworlds* 2004, November in Japan. ISBN 0-7695-2140-1.

[2] Ramos, Félix F, Luis Razo, Alma V. Martínez, Fabiel Zúñiga y Hugo I. Piza. 3D Emotional Agent Architecture. Innovative Internet Community Systems, Lecture Notes in Computer Science, vol. 3908/2006, ISBN 978-3-540-33973-1, pp. 181-194.

[3] Zuñiga, Fabiel, Félix Ramos e Iván Piza. *Specifying Agent's Goals in 3D Scenarios Using Process Algebras*. Springer LNC 3563 2005, ISBN 3-540-28063-4, ISSN 0302-9743.

[4] López, E. "Multi-Level Modeling of Multi-Mobile Agent Systems", cap. XIII, en X. Zha (ed.). *Artificial Intelligence and Integrated Intelligent Information Systems: Emerging Technologies and Applications*. ISBN: 1-59904-249-5, Idea Group, Inc pp.256-277 Oct. 2006.

[5] Flores, M., M. Padilla y E. López. Modeling and Simulation of mobile agents systems using a multi-level net formalism. Mexican International Conference on Artificial Intelligence (MICAI 2006). Lecture Notes in Computer Science 4293, Springer, pp.1128-1138. ISSN 0302-9743 Apizaco, Mexico, noviembre 2006.

[6] Ramírez, A., E. Ruiz, I. Rivera y E. López. Diagnosability and Fault Location of Discrete Event Systems. A Petri Net Based Approach. *IEEE Transactions on Automation Science and Engineering*, vo1. 4-1, pp. 31-39. Enero 2007.

[7] Leiner, B.M., V.G. Cerf, D.D. Clark, R.E. Kahn, L. Kleinrock, D. C. Lynch, J. Postel, L.G. Roberts y S. Wolff. *A brief history of the internet*. Internet Society. 2003.

[8] Psounis, K. Active networks: Applications, security, safety, and architectures. *IEEE Communications Surveys*, vol. 2, núm. 1, pp. 2-16, 1999.

[9] Siller, M. y J. Woods. Using an Agent Based Platform to Map Quality of Service to Experience in Conventional and Active Networks. *Journal IEE Proceedings - Communications*, vol. 153, núm. 6, pp. 828-840, 2006. 1350-2425.

[10] Stepinski, T.F. y R. Vilalta. Digital Topography Models for Martian Surfaces. *IEEE Geoscience and Remote Sensing Letters*, 2(3), pp. 260-264, 2005.

[11] Stepinski, T.F., S. Ghosh y R. Vilalta. Automatic Recognition of Landforms on Mars Using Terrain Segmentation and Classification. International Conference on Discovery Science 2006 , N. Lavrac; L. Todorovski; K.P. Jantke, Eds., LNAI 4265, pp. 255-266, 2006.

[12] Vilalta, R., T.F. Stepinski y M. Achari. An Efficient Approach to External Cluster Assessment with an Application to Martian Topography. *Journal of Data Mining and Knowledge Discovery*, 2007.

[13] Clarke, E., D. Peled y O. Grumberg. *Model Checking*. MIT Press, 2000.

[14] Ziller, Roberto y Klaus Schneider. Combining Supervisor Synthesis and Model Checking, *ACM Transactions on Embedded Comp. Sys.*, vol. 4, núm. 2, 2005.

Computación cuántica: un esbozo de sus métodos y desarrollos

UNA VISIÓN PANORÁMICA DE LA NOCIÓN DE COMPUTACIÓN CUÁNTICA: SUS ELEMENTOS MATEMÁTICOS BÁSICOS, LAS VENTAJAS QUE IMPLICA EN COMUNICACIONES Y CRIPTOGRAFÍA, ASÍ COMO ALGUNAS OPCIONES ACTUALES PARA SU IMPLEMENTACIÓN.

Guillermo Morales-Luna

Ignoranti quem portum petat nullus suus ventus est.
(Nunca hay viento favorable para quien ignora hacia cuál puerto se dirige.)
Séneca

Elementos matemáticos básicos

En la mecánica cuántica, uno de los elementos más importantes es la noción de *estados de energía*. Estos son puntos en un espacio lineal generado por las funciones propias de un operador hamiltoniano, según lo describe la *ecuación de Schrödinger*, y son *unitarios*, es decir, su longitud euclidiana, vistos como elementos del espacio, es 1. Toda combinación lineal de las funciones propias, que sea unitaria, se ve como una superposición de las funciones propias y la probabilidad de que el estado asuma una de ellas es el cuadrado del valor absoluto de su coordenada en la dirección de esa función propia. En resumen, *la probabilidad de que el estado asuma una dirección es el cuadrado de su amplitud en esa dirección.*

Tal idea ha dado origen al *cómputo cuántico*. Los bits clásicos 0 y 1 se ponen en correspondencia con dos vectores unitarios en un espacio vectorial sobre los números complejos y cada vector unitario en ese espacio se ve como la superposición de esos dos bits. Se conviene en que, para una tal superposición, una *medición* la hará asumir uno de los dos valores, 0 ó 1, es decir, una de las dos direcciones básicas, con la probabilidad dada por el cuadrado de su amplitud en esa dirección.

Los *operadores primitivos* en el cómputo cuántico son las transformaciones unitarias; es decir, son transformaciones lineales cuyas inversas son sus propias transpuestas conjugadas, y en esto se sigue también una motivación de la mecánica cuántica. Un algoritmo cuántico es una lista de operadores primitivos, compuestos de manera consecutiva junto con toma de mediciones. Como todo paradigma de cómputo, el cómputo cuántico calcula funciones. Una función es *calculable* por un algoritmo cuántico si para cualquier entrada, es decir una cadena de bits, el algoritmo termina dando como salida el valor de

GUILLERMO MORALES-LUNA Es licenciado en Física y Matemáticas (ESFM-IPN), maestro en Ciencias con especialidad en Matemáticas (**Cinvestav**) y doctor en Ciencias Matemáticas (Instituto de Matemáticas, Academia Polaca de Ciencias). Ocupa el cargo de Investigador Titular en el Departamento de Computación del **Cinvestav**. Sus áreas de interés son: fundamentos matemáticos de computación; lógica y deducción automática; criptografía y teoría de la complejidad. Ha sido profesor en el IPN y en la B. Universidad Autónoma de Puebla. Ha realizado dos estancias sabáticas en el Instituto Mexicano del Petróleo. Es mexicano por nacimiento y también le fue conferida la ciudadanía polaca.
gmorales@cs.cinvestav.mx

la función en la entrada, codificada como una lista de bits, con una probabilidad 1.

Los textos clásicos en este tema son [2] y [10]. A diferencia de los conceptos básicos de información clásica, el bit que puede asumir valores 0 ó 1, y los bits pueden concatenarse para formar arreglos de crecimiento lineal, en el cómputo cuántico la unidad básica, el *qubit*, puede estar en una superposición de valores 0 y 1, y al concatenar a los qubits, se forman arreglos de crecimiento exponencial. Esto dota al cómputo cuántico de un paralelismo inherente que permite acelerar notoriamente los procesos. A continuación se expone una breve cronología de la computación cuántica.

La idea de computación cuántica se desarrolló en la segunda mitad del siglo XX. Rolf Landauer, científico de origen alemán, radicado en los EUA desde la década de 1930, y que laboraba en IBM, planteó en 1961 que la información tiene una manifestación física: cuando se pierde en un circuito irreversible, la información se convierte en entropía y se disipa como calor. En contraposición, los circuitos reversibles, desde el punto de vista físico, son aquéllos que no incrementan la entropía, por lo que poseen una mayor eficiencia de la energía y, desde el punto de vista lógico, son aquéllos en los que cada operador primitivo actúa de manera inyectiva. Todo circuito reversible en el sentido lógico lo es en el sentido físico. Desde la década de 1970, Charles Bennet, también de IBM, en el centro Thomas Watson ha estudiado la noción de *reversibilidad* de las computaciones. En 1981, Richard Feynman planteó que los sistemas físicos, incluidos los de nivel cuántico, podían ser simulados de manera exacta por computadoras cuánticas. En 1982, Peter Beniof, del Laboratorio Nacional de Argonne, presentó modelos lógicos de máquinas de Turing cuánticas, y en 1984, Charles Bennet y Gilles Brassard, éste último de la Universidad de Montreal, introdujeron las nociones básicas de criptografía cuántica. En 1985, David Deutsch, de la Universidad de Oxford, reinterpretó la llamada Tesis de Church-Turing en el marco del cómputo cuántico y, desde 1993, Bennet, Brassard, Crepeau, Josza, Peres y Wooters han desarrollado el uso de la noción de *teleportación*. En 1994, Peter Shor, entonces en ATT, publicó su célebre algoritmo cuántico para factorizar enteros.

La unidad básica de información en el cómputo cuántico es, entonces, el *qubit*, en contraposición del *bit clásico*. Denotemos por Q al espacio de qubits y por $B = \{0,1\}$ al de los bits clásicos. La noción de *superposición* se realiza en el ambiente de *espacios de Hilbert*. Formalmente, los qubits son vectores unitarios en un espacio complejo

de dimensión 2 sobre los complejos, es decir, $\mathbf{Q}$ es la esfera unitaria del espacio vectorial $\mathbf{C}^2$. Si $x = x_0\mathbf{e}_0 + x_1\mathbf{e}_1 = [x_0 \;\; x_1]^T$ es un qubit,

$x_0, x_1 \in \mathbf{Q}$, $|x_0|^2 + |x_1|^2 = 1$, se escribe de acuerdo con la notación debida a Dirac, $\mathbf{x} = x_0|0\rangle + x_1|1\rangle$. Los bits clásicos se identifican, respectivamente, con $0 \leftrightarrow |0\rangle = [1 \;\; 0]^T$ y $1 \leftrightarrow |1\rangle = [0 \;\; 1]^T$.
Al *tomar una medición* el qubit $\mathbf{x}$ asumirá el valor $|0\rangle$ con probabilidad $|x_0|^2$ y el valor $|1\rangle$ con probabilidad $|x_1|^2 = 1 - |x_0|^2$. Así, la probabilidad de que el qubit asuma el valor "cero" es el cuadrado del valor absoluto de la primera coordenada, $\Pr(\mathbf{x} \to |0\rangle) = |x_0|^2$ y la probabilidad de que asuma el valor "uno" es la complementaria, $\Pr(\mathbf{x} \to |1\rangle) = |x_1|^2$. En tanto que no se tome la medición, cada qubit es una superposición de los dos básicos $|0\rangle$ y $|1\rangle$.

La esfera unitaria del espacio complejo $\mathbf{C}^2$ es una variedad de dimensión 3, sobre los números reales, por lo que puede ser parametrizada de manera alternativa considerando tres coordenadas, dos de los cuales son los ángulos θ y φ. Mediante las correspondencias

$$\begin{aligned} x_0 &\leftrightarrow \cos\frac{\theta}{2} \\ x_1 &\leftrightarrow e^{i\varphi}\operatorname{sen}\frac{\theta}{2} \\ \mathbf{x} = x_0|0\rangle + x_1|1\rangle &\leftrightarrow \cos\frac{\theta}{2}\,|0\rangle + e^{i\varphi}\operatorname{sen}\frac{\theta}{2}\,|1\rangle \end{aligned}$$

se identifica a la sección de la esfera de qubits correspondiente a abscisas con valores reales con la llamada *esfera de Bloch*. Ésta es una representación geométrica de uso común en cómputo cuántico.

Los *quregistros*, no son sólo concatenaciones de qubits, sino que son productos tensoriales de ellos, por lo que la dimensión de los quregistros crece exponencialmente respecto al número de qubits concatenados. Si $\mathbf{x}_0, \ldots, \mathbf{x}_{n-1} \in \mathbf{Q}$ son n qubits, su correspondiente *n-quregistro* es $\mathbf{x} = \mathbf{x}_0 \otimes \ldots \otimes \mathbf{x}_{n-1} \in \mathbf{C}^{2^n}$. Si $\mathbf{Q}^n$ es la colección de n-quregistros, entonces $\mathbf{Q}^n$ es la esfera unitaria del espacio complejo $\mathbf{H}_n$ de dimensión 2^n, la cual es precisamente la cardinalidad de $\mathbf{B}^n$. Para cada $j = 0, \ldots, 2^n - 1$, se escribe $\mathbf{e}_j = |(j)_2\rangle = |\varepsilon\rangle$ donde $\varepsilon = (j)_2$ es la representación en base 2 de j, de longitud n. La base canónica del espacio $\mathbf{H}_n$ es pues $(|\varepsilon\rangle)_{\varepsilon \in \mathbf{B}^n}$. Por ejemplo, para n=3, $\mathbf{H}_3 = \mathbf{C}^8$ y su base canónica es

$$\{\mathbf{e}_j\}_{j=0}^{7} = \{|000\rangle, |001\rangle, |010\rangle, |011\rangle, |100\rangle, |101\rangle, |110\rangle, |111\rangle\}$$

Las operaciones básicas son matriciales y en un solo paso de cómputo afectan a un número exponencial de componentes. Como deben de transformar quregistros en quregistros, necesariamente han de ser unitarias. Si $U : \mathbf{H}_1 \to \mathbf{H}_1$ es una transformación lineal unitaria, es decir $U^{-1} = U^H$, donde esta última es la conjugada transpuesta, o *hermitiana*, de la matriz U, entonces se dice ser una *compuerta cuántica* o *qucompuerta*. Para dos qucompuertas $U, V : \mathbf{H}_1 \to \mathbf{H}_1$, su *producto tensorial* es $U \otimes V : \mathbf{H}_2 \to \mathbf{H}_2$ tal que $(U \otimes V)(\mathbf{x} \otimes \mathbf{y}) = U(\mathbf{x}) \otimes V(\mathbf{y})$.

Sucesivamente, se define $U^{\otimes 1} = U$ y $U^{\otimes(n+1)} = U \otimes U^{\otimes n}$.

Las siguientes son matrices unitarias:

$$\sigma_0 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \sigma_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad \sigma_y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \quad \sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

donde $i = \sqrt{-1}$, y se dicen ser las *matrices de Pauli*. La primera es la matriz identidad 1_2, la segunda es una *negación*, la cuarta es un *cambio de fase*. La tercera hace las veces de una negación y de un cambio de fase.

Otra compuerta cuántica importante es la *transformación de Hadamard*:

$$H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix},$$

cuyo efecto es que si $\mathbf{x} = x_0|0\rangle + x_1|1\rangle$

entonces

$$H\mathbf{x} = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}\begin{bmatrix} x_0 \\ x_1 \end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix} x_0 + x_1 \\ x_0 - x_1 \end{bmatrix} = \frac{x_0 + x_1}{\sqrt{2}}|0\rangle + \frac{x_0 - x_1}{\sqrt{2}}|1\rangle$$

es decir, el operador de Hadamard "promedia" las coordenadas.

Una función booleana, es decir, que transforma señales de 0's y 1's en otras señales de 0's y 1's, $f : \mathbf{B}^n \to \mathbf{B}^m$ puede ser confundida con la transformación lineal entre espacios vectoriales $U_f : \mathbf{H}^{n+m} \to \mathbf{H}^{n+m}$ tal que $|\varepsilon\rangle|\delta\rangle \mapsto |\varepsilon\rangle|\delta \oplus f(\varepsilon)\rangle$. Esta transformación actúa como una mera permutación de los vectores básicos y es por tanto unitaria. Si n=m=1 entonces

$$\begin{aligned} U_f(H\mathbf{x} \otimes |0\rangle) &= \frac{x_0 + x_1}{\sqrt{2}}U_f(|0\rangle \otimes |0\rangle) + \frac{x_0 - x_1}{\sqrt{2}}U_f(|1\rangle \otimes |0\rangle) \\ &= \frac{x_0 + x_1}{\sqrt{2}}|0f(0)\rangle + \frac{x_0 - x_1}{\sqrt{2}}|1f(1)\rangle \end{aligned}$$

en otras palabras, $U_f(H\mathbf{x} \otimes |0\rangle)$ está dando "sendos promedios de los valores de f". Para n, m cualesquiera, la matriz $H^{\otimes n}$ es de orden $(2^n \times 2^n)$, y se tiene similarmente que $U_f(H^{\otimes n}\mathbf{x} \otimes |0\rangle)$ está dando "promedios de los valores de f": cada valor $|\delta f(\delta)\rangle$ será asumido con una probabilidad dada por el valor $2^{-n}\left[\sum_{\varepsilon \in \mathbf{B}^n} h_{\delta\varepsilon}x_\varepsilon\right]^2$.

Así vemos que el cómputo cuántico, en un número "lineal" de pasos, conlleva la información de un número "exponencial" de posibles valores.

Procedimientos de comunicaciones y de criptografía

En comunicaciones, la computación cuántica proporciona, además, disminución de costos debido al fenómeno de entrelazamiento (*entanglement*, en inglés).

Entrelazamiento

La colección de 2-quregistros es la esfera unitaria en $H_2 = C^{2^2} = C^4$. Dado un quregistro $x^{(2)} = x_{00}|00\rangle + x_{01}|01\rangle + x_{10}|10\rangle + x_{11}|11\rangle \in Q^2$ se tendrá que la probabilidad de que el quregistro asuma una de las cuatro posibles palabras de dos bits es $\Pr(x^{(2)} \to |ij\rangle) = |x_{ij}|^2$, para cada $i, j \in \{0,1\}$. Sin embargo, si se toma una medición en el primer qubit y éste asume el valor $i \in \{0,1\}$ entonces el 2-quregistro tomará el valor

$$x^{(2)}\Big|_{x_0 \to |i\rangle} = \frac{1}{\sqrt{|x_{i0}|^2 + |x_{i1}|^2}}\left(x_{i0}|i0\rangle + x_{i1}|i1\rangle\right),$$

es decir, el segundo qubit se mantiene en una superposición. Similarmente, si se mide al segundo qubit y éste asume el valor $j \in \{0,1\}$ entonces el 2-quregistro tomará el valor

$$x^{(2)}\Big|_{x_1 \to |j\rangle} = \frac{1}{\sqrt{|x_{0j}|^2 + |x_{1j}|^2}}\left(x_{0j}|0j\rangle + x_{1j}|1j\rangle\right),$$

es decir, el primer qubit se mantiene en una superposición. Sin embargo, supongamos

$$[x_{00} \quad x_{01} \quad x_{10} \quad x_{11}] = \left[\frac{1}{\sqrt{2}} \quad 0 \quad 0 \quad \frac{1}{\sqrt{2}}\right].$$

Entonces, resulta $x^{(2)}\Big|_{x_0 \to |i\rangle} = |i\bar{i}\rangle$

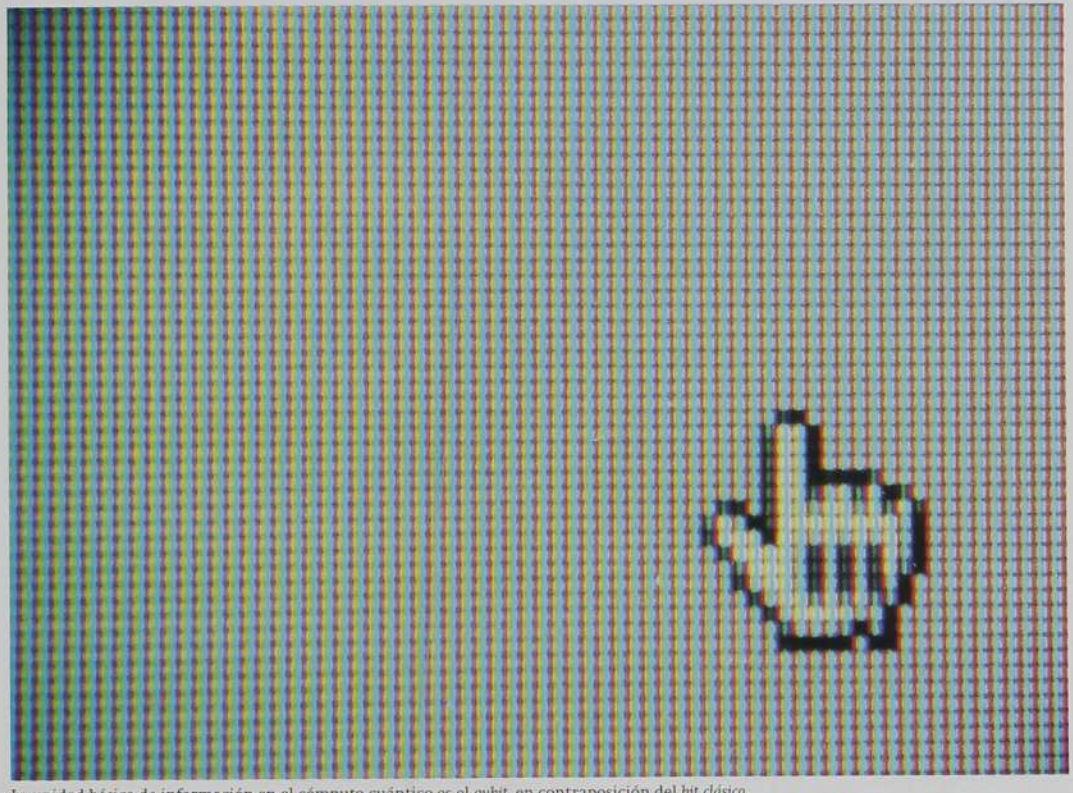
y $x^{(2)}\Big|_{x_1 \to |j\rangle} = |jj\rangle$, es decir, una vez que se determina un qubit, el otro queda también determinado, con el mismo valor. Similarmente, supongamos

$$[x_{00} \quad x_{01} \quad x_{10} \quad x_{11}] = \left[0 \quad \frac{1}{\sqrt{2}} \quad \frac{1}{\sqrt{2}} \quad 0\right].$$

Entonces, resulta $x^{(2)}\Big|_{x_0 \to |i\rangle} = |i\bar{i}\rangle$

y $x^{(2)}\Big|_{x_1 \to |j\rangle} = |\bar{j}\bar{j}\rangle$, es decir, una vez que se determina un qubit, el otro queda también determinado, con el valor opuesto.

En estos casos se tiene que ambos qubits están entrelazados: el valor que asuma uno, determinará el que ha de asumir el otro.



La unidad básica de información en el cómputo cuántico es el *qubit*, en contraposición del *bit clásico*.

Consideremos ahora, $b_{00}=\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)$,

$b_{01}=\frac{1}{\sqrt{2}}(|01\rangle+|10\rangle)$,

$b_{10}=\frac{1}{\sqrt{2}}(|00\rangle-|11\rangle)$ y

$b_{11}=\frac{1}{\sqrt{2}}(|01\rangle-|10\rangle)$.

La colección $\{b_{00},b_{01},b_{10},b_{11}\}$ es una base ortonormal, llamada *de Bell*, del espacio de 2-quregistros H_2. De hecho, $b_{ij}=C(H\otimes 1_2)(|i\rangle\otimes|j\rangle)=C(H|i\rangle\otimes|j\rangle)$, donde C es la compuerta *NO-Controlado*, $C:|00\rangle\mapsto|00\rangle,|01\rangle\mapsto|11\rangle,|10\rangle\mapsto|10\rangle,|11\rangle\mapsto|01\rangle$ (si el segundo bit es 0 deja el primero intacto, pero si es 1 "niega" al primero). Considerando las matrices de Pauli, se puede ver que también valen las igualdades: $b_{00}=(1_2\otimes 1_2)b_{00}$, $b_{01}=(\sigma_x\otimes 1_2)b_{00}$, $b_{10}=(\sigma_z\otimes 1_2)b_{00}$, $b_{11}=(\sigma_z\sigma_x\otimes 1_2)b_{00}$.

Protocolos de comunicación

El entrelazamiento produce diferencias notorias respecto al cómputo clásico: Supongamos un protocolo que involucra dos partes *Alicia* y *Beto* que se han de comunicar bits clásicos. Ellos reciben sendos bits ε_A y ε_B y han de producir bits a y b tales que $\varepsilon_A\wedge\varepsilon_B=a\oplus b$.

Por un lado, tenemos que $\varepsilon_A\wedge\varepsilon_B$ es 1 sólo en una de sus cuatro posibilidades, en tanto que $a\oplus b$ es 1 en dos de sus cuatro posibilidades. Así, la mejor estrategia de Alicia y Beto es lograr $a=b$, con lo cual $a\oplus b=0$, y la probabilidad de éxito es entonces 3/4. Las partes necesitan pues comunicarse un bit clásico para tener éxito con probabilidad 3/4.

Para la implementación cuántica, consideremos el 2-quregistro

$$x_0x_1=x^{(2)}=\frac{1}{\sqrt{2}}(|00\rangle-|11\rangle)$$

que consta de dos qubits entrelazados: el valor que tome uno en una medición lo ha de tomar el otro. El primer qubit queda en posesión de Alicia y el segundo en el de Beto. Consideremos la matriz correspondiente a la rotación de $\frac{\pi}{8}$ radianes:

$$G=\begin{bmatrix}\cos\left(\frac{\pi}{8}\right) & \operatorname{sen}\left(\frac{\pi}{8}\right)\\ -\operatorname{sen}\left(\frac{\pi}{8}\right) & \cos\left(\frac{\pi}{8}\right)\end{bmatrix}.$$

Sean $M_A=\begin{cases}1_2 & \text{si } \varepsilon_A=0\\ G & \text{si } \varepsilon_A=1\end{cases}$,

$$M_B=\begin{cases}1_2 & \text{si } \varepsilon_B=0\\ G^T & \text{si } \varepsilon_B=1\end{cases}.$$

Alicia produce su bit tomando como a el resultado de tomar medición a M_Ax_0 y Beto produce su bit tomando como b el resultado de tomar medición a M_Bx_1. Se puede ver que $\Pr(a\oplus b\neq\varepsilon_A\wedge\varepsilon_B)=\sum_{\varepsilon_A,\varepsilon_B\in B}\frac{1}{4}\Pr(a\oplus b\neq\varepsilon_A\wedge\varepsilon_B|\varepsilon_A,\varepsilon_B)=\frac{3-\sqrt{2}}{8}$,

por tanto, la probabilidad de éxito en el protocolo es la complementaria,

$$1-\left(\frac{3-\sqrt{2}}{8}\right)=\frac{5+\sqrt{2}}{8}\approx 0.80177...$$

Así pues, con entrelazamiento solamente y sin necesidad de transmitir ningún bit, la probabilidad de éxito es mayor que en el enfoque clásico.

Otra aplicación importante del entrelazamiento es la llamada *supercodificación*: una parte, *Alicia*, ha de comunicar una pareja de bits clásicos $\varepsilon_0\varepsilon_1\in B^2$ a otra parte, *Beto*. Supongamos que se prepara el 2-quregistro entrelazado

$$x_0x_1=b_{00}=\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle),$$

y se da el primer qubit x_0 a Alicia y el segundo x_1 a Beto. En función de la pareja $\varepsilon_0\varepsilon_1$, Alicia toma un operador U_A para aplicar sobre su qubit:

$$\begin{aligned}\varepsilon_0\varepsilon_1=00 &\Rightarrow U_A=\sigma_0=1_2\\ \varepsilon_0\varepsilon_1=01 &\Rightarrow U_A=\sigma_x\\ \varepsilon_0\varepsilon_1=10 &\Rightarrow U_A=\sigma_z\\ \varepsilon_0\varepsilon_1=11 &\Rightarrow U_A=\sigma_z\sigma_x\end{aligned}$$

Alicia produce $y_0=U_Ax_0$ y se lo envía a Beto. Observemos aquí, que necesariamente se ha de tener $(U_A\otimes 1_2)b_{00}=b_{\varepsilon_0\varepsilon_1}$.
Beto entonces calcula $z=(H\otimes 1_2)C(y_0\otimes x_1)$ y al tomar una medición respecto a la base de Bell recuperará $\varepsilon_0\varepsilon_1$ pues *a fortiori* $z=b_{\varepsilon_0\varepsilon_1}$.

Así pues, basta con la transmisión de un solo qubit para codificar dos bits clásicos.

Procedimientos de criptografía

En criptografía, el cómputo cuántico ha permitido diversos protocolos para el establecimiento de claves comunes. Una característica de ellos es que es incluso posible detectar la sola presencia de un intruso.

Sea $E^0=\{e_0^0,e_1^0\}=\{|0\rangle,|1\rangle\}$ la base canónica de H_1 y sea $H(E^0)=E^1=\{e_0^1,e_1^1\}=\{H|0\rangle,H|1\rangle\}$ la base de H_1 obtenida al aplicar la transformación de Hadamard a E^0, la cual puede corresponder a un *spin* con polarización *vertical-horizontal*, $E^0=\{\uparrow,\rightarrow\}$, y E^1 a un *spin* con polarización *oblicua, NO-NE*, $E^1=\{\nwarrow,\nearrow\}$.

Dos partes, Alicia y Beto, han de establecer una clave común. Cuentan con dos canales de transmisión

Canal cuántico. Transmite de manera unidireccional, digamos de Alicia hacia Beto.

Canal clásico. Transmite de manera bidireccional.

Supongamos que la transmisión a través de los canales está libre de cualquier ruido.

Protocolo sobre el canal cuántico

1. Alicia genera dos sucesiones de bits $\delta = [\delta_i]_{i=1}^{N}$ y $\varepsilon = [\varepsilon_i]_{i=1}^{N}$.

   Transmite por el canal cuántico la sucesión de estados $S = \left[s_i = e_{\varepsilon_i}^{\delta_i}\right]_{i=1}^{N}$.

2. Beto genera una sucesión de bits $\eta = [\eta_i]_{i=1}^{N}$ y realiza una medición de cada qubit s_i respecto a la base E^{η_i} para obtener así una sucesión de bits $\zeta = [\zeta_i]_{i=1}^{N}$. Toda vez que $\varepsilon_i = \eta_i$, se va a tener que $\delta_i = \zeta_i$, por lo que puede esperarse que en casi $N/2$ entradas van a coincidir las sucesiones δ y ζ.

Protocolo sobre el canal clásico

1. Beto le envía su sucesión ζ a Alicia.
2. Alicia calcula el conjunto $J = \{i \leq N \mid \zeta_i = \varepsilon_i\}$ que corresponde a cuando Beto seleccionó la base correcta. Alicia le envía, de vuelta, J a Beto.
3. Necesariamente, las restricciones de δ y de ζ a J, $\delta|_J$ y $\zeta|_J$ han de coincidir, $\forall j \in J : \delta_j = \zeta_j$, y por tanto esa sucesión, o una porción de ella, puede ser asumida como la llave en común. La única manera en la que δ y ζ podrían diferir sería mediante la intromisión de una tercera parte, Isabel.
4. Para revisar si acaso hubo una intromisión, Alicia y Beto intercambian porciones de sus respectivas sucesiones $\delta|_J$ y $\zeta|_J$. Cada vez que intercambian una porción, la suprimen de sus sucesiones. Si en alguna pareja de porciones intercambiadas aparece una discrepancia, se detecta la intromisión de Isabel. De otra manera, se puede confiar, con una muy alta probabilidad, que la llave en común ya ha sido establecida.

Estos protocolos ya están siendo distribuidos comercialmente; por ejemplo, existe una compañía, MagiQ Technologies, Inc. con base en Boston.

Implementaciones actuales

En cuanto a la implementación, se tiene que cualquier sistema físico que realice la computación cuántica ha de cumplir con los criterios siguientes, llamados *de DiVicenzo*:

1. Tener caracterizada la noción de qubit y poder ensamblar varios de ellos.
2. Contar con un conjunto de compuertas cuánticas primitivas que permitan realizar cualquier algoritmo.
3. Poder inicializar una lista de qubits en estados puros determinados.
4. Poder ejecutar la operación de toma de mediciones.
5. Que los tiempos de decoherencia excedan los de aplicación de las compuertas cuánticas primitivas.

Ha habido varios modelos físicos [5]:

- **Resonancia nuclear magnética** *(Nuclear Magnetic Resonance, NMR).* Un conjunto de moléculas en una solución líquida en el que siete *espines* en cada molécula hacen las veces de siete qubits [12]. Con esto se puede factorizar a 15 como el producto de 3 por 5. Sin embargo, no podría extenderse el modelo a más de 10 qubits.
- **Cavidad electrodinámica cuántica** *(Cavity Quantum Electro-Dynamics, Cavity QED).* Consiste de la interacción entre un qubit material (realizado como un átomo atrapado o un sistema puntual *-dot-* semiconductor) y un campo cuantizado -propiamente un fotón- de un resonador de microondas. A fin de conseguir una dinámica coherente, se utiliza una *cavidad* para ampliar la frecuencia coherente de Rabi entre el átomo y el campo. Este modelo es apropiado para convertir estados de qubits materiales y qubits de fotones y es particularmente apto para protocolos de 2-qureg istros [4]; también ha sido utilizado en protocolos de comunicación, destacándose en ello el grupo del profesor catalán J.I. Cirac [3] del Instituto Max Planck.
- **Trampas de iones** *(Ion Trap).* Se utilizan arreglos de trampas de iones interconectados por fotones, o por iones que hacen las veces de cabezas lectoras para transmitir la información entre arreglos, o por iones que transitan entre los arreglos. Los qubits dados como iones se mueven en diferentes zonas de trampas sin decoherencia

La idea de computación cuántica se desarrolló en la segunda mitad del siglo XX. Rolf Landauer, científico de origen alemán, planteó en 1961 que la información tiene una manifestación física; es decir, cuando se pierde en un circuito irreversible, la información se convierte en entropía y se disipa como calor.

en tiempos adecuados para la aplicación de compuertas cuánticas [9]. Las trampas pueden realizarse como sistemas micro-electro-mecánicos o mediante técnicas de nanofabricación.

- **Átomos neutros** *(Neutral atoms)*. Un sistema de átomos neutros atrapados puede ser apropiado para el cómputo cuántico debido a una estructura atómica simple al nivel cuántico, a que se mantienen aislados del medio ambiente y a su habilidad para atrapar e interactuar con una gran cantidad de átomos idénticos. Una computadora cuántica podría ser vista como un reloj atómico que consiste de varios átomos que interactúan de manera controlada. En la actualidad existen niveles de control para producir condensados de Bose-Einstein [1] y gases degenerados de Fermi, con lo cual se ha previsto acoplar átomos.
- **Técnicas ópticas.** Comenzaron a utilizarse en protocolos criptográficos y para realizar el fenómeno de entrelazamiento [11] y han sido muy importantes en la investigación del procesamiento cuántico de la información. Aunque han mostrado se eficacia en protocolos de comunicación, se tiene el problema de "escalabilidad": hay limitaciones para formar ensambles de qubits fotónicos, aunque acaso éstas no sean esenciales [7]. La detección de efectos no-lineales entre fotones abre una posibilidad de "escalar" el modelo.
- **Superconductividad.** Aquí los qubits son circuitos de superconductividad operando a temperaturas de miligrados Kelvin [8]. Por ser de tipo eléctrico, pueden interactuar con transistores consistentes de un solo electrón. Los qubits se inicializan enfriando los sistemas a su estado base. Entonces, mediante pulsos electromagnéticos de radio-frecuencia se aplican las operaciones cuánticas. Se puede tener velocidades del orden de 700 GHz con muy poca disipación de potencia. Las mediciones respecto a diversas bases pueden ser realizadas mediante magnetómetros de interferencia cuántica de superconductividad.
- **Técnicas de estado sólido.** En éstas [6], los qubits son sistemas de dos niveles altamente coherentes correspondientes a estados de *espines* de electrones localizados o de núcleos atómicos. Las compuertas quedan dadas por interacciones recíprocas entre los *espines*. Las transiciones excitónicas ortogonalmente polarizadas pueden realizar la noción de una pareja de qubits y el emparejamiento coulombiano de alto-orden, que conlleva la formación bi-excitónica, puede utilizarse para realizar la noción de entrelazamiento. Una limitación de este enfoque son los cortos tiempos de decoherencia.

Un problema algorítmico abierto

Las comunicaciones actuales se han automatizado rápidamente y los procesos involucrados se utilizan de manera cada vez más extensa y compleja. Actividades como búsqueda de información, el intercambio de datos con el propósito de realizar protocolos, o la revisión de privilegios y autorizaciones otorgados por terceras partes, son comunes en transacciones comerciales, bancarias, contables, legales o de simple entretenimiento. Esto ha propiciado el desarrollo de

Las comunicaciones actuales se han automatizado rápidamente y los procesos involucrados se utilizan de manera cada vez más extensa y compleja

la seguridad informática. Los procesos electrónicos de autentificación y cifrado son de suma importancia en la sociedad moderna. Aunque éstos pueden dotar de una cierta "identidad" a los agentes informáticos y a sus propietarios (los métodos de autentificación conllevan procesos de no-repudio incontrovertibles), la autonomía de las partículas de *software* está aún muy restringida. La llamada criptografía de clave pública ha facilitado el establecimiento de claves privadas propias de cada transacción y se usa en el protocolo de comunicaciones SSL (*Secure Socket Layer*) de Internet. Sus protocolos se basan en problemas matemáticos de gran dificultad, tales como el de factorización de enteros, a saber, encontrar los factores primos de un número entero muy grande (del orden de 1 024 o 2 048 bits cuando se le escribe en binario), o del cálculo de logaritmos discretos, es decir, en un grupo cíclico, dado un generador de él, para un elemento cualquiera se trata de encontrar la mínima potencia del generador que lo representa. Las dificultades de estos problemas son aparentemente esenciales, por lo que nuevos dispositivos de cálculo sólo acelerarían en factores constantes el desempeño de los algoritmos para resolverlos. El cómputo cuántico, sin embargo, por la posibilidad de involucrar en un solo paso de cómputo una cantidad exponencial de información, podría disminuir la complejidad de los algoritmos para resolverlos. Por ejemplo, el mejor algoritmo para resolver el problema de factorización tiene una complejidad subexponencial (su orden es una potencia de la raíz cúbica del número de bits de la instancia), mientras que el algoritmo cuántico de Shor [10], para resolverlo, tiene una complejidad polinomial, de orden cúbico, pero involucra un orden lineal de qubits respecto al número de bits con los que se escriba el entero a factorizar. El modelo NMR de computadoras cuánticas [12] no significa ningún riesgo para los protocolos actuales. El problema de factorización, y su complemento, el decidir si un entero es un primo, están en la clase de problemas NP. Aún en la actualidad no se sabe si alguno de ellos es completo en esa clase, es decir, cualquier otro problema ahí se reduce procedimentalmente al problema de factorización, y se sospecha que no lo es, pues si lo fuera, se tendría que la clase NP sería cerrada por complementos, algo que la experiencia hace intuir que no es verdad, aunque esto último no ha sido tampoco demostrado.

El algoritmo de Shor, publicado hace ya 13 años, hace que la computación cuántica sea vista como un elemento que habrá de desafiar a los protocolos de comunicación en boga, cuando las limitaciones tecnológicas actuales hayan sido superadas. Luego de resolver el problema de factorización, el problema del logaritmo discreto también podría resolverse eficientemente mediante un algoritmo cuántico que utiliza la parte medular del algoritmo de Shor: el cálculo de órdenes de elementos en un grupo cíclico. Es, por tanto, del interés fundamental de la criptografía desarrollar métodos robustos ante los procedimientos para resolver los problemas de factorización y del logaritmo discreto. En el cómputo cuántico se ha planteado un problema matemático muy importante, el llamado *problema del subgrupo escondido*. Dado un grupo G y un subgrupo H contenido en él, una función f definida en G se dice que *separa clases* de H si dos elementos en G poseen una misma imagen bajo f si y sólo si sus clases módulo H coinciden, en símbolos: $\forall x_0, x_1 \in G$, $f(x_0) = f(x_1) \iff x_0 H = x_1 H$. El problema está en que, dada una función f que separa algún subgrupo (escondido), es necesario caracterizar a ese subgrupo (es decir, calcular un conjunto de generadores) utilizando el menor número de evaluaciones de la función f. Ambos problemas, el de factorización y el del logaritmo discreto, se reducen al problema del subgrupo escondido. En la actualidad se trabaja en diseñar un algoritmo cuántico de tiempo polinomial en la descripción del grupo y de la función.

La computación cuántica, entonces, es todavía un paradigma lógicamente viable que no ha sido implementado a plenitud debido a limitaciones tecnológicas. En un plazo de unas dos décadas seguramente presenciaremos avances notables en ello. ●

[Referencias]

[1] J.R. Anglin y W. Ketterle. Bose-Einstein condensation of atomic gases. *Nature*, 416:211-218, 2002.

[2] Dirk Bouwmeester, Artur Ekert, y Anton Zeilinger (eds.). *The Physics of Quantum Information*. Springer-Verlag, 2000.

[3] H.J. Briegel, J.I. Cirac, W. Dür, S.J. van Enk, H.J. Kimble, H. Mabuchi y P. Zoller. Physical implementations for quantum communication in quantum networks. *Quantum Computing and Quantum Communications*, 1509:373-382, 1999.

[4] L.M. Duan, A. Kuzmich, and H.J. Kimble. Cavity QED and quantum-information processing with "hot" trapped atoms. *Physical Review A*, 67:032305, 2003.

[5] Richard Hughes and Todd Heinrichs. Quantum information science and technology roadmap. 2004. disponible en http://qist.lanl.gov/.

[6] D. Loss y D.P. DiVincenzo. Quantum computation with quantum dots. *Physical Review A*, 57:120-126, 1998.

[7] M.D. Lukin y A. Imamoglu. Nonlinear optics and quantum entanglement of ultraslow single photons. *Physical Review Letters*, 84:1419-1422, 2000.

[8] Y. Maklin, G. Schön, y A. Shnirman. Quantum-state engineering with Josephson junction devices. *Reviews of Modern Physics*, 73:357, pp. 400, 2001.

[9] C. Monroe. Quantum information processing with atoms and photons. *Nature*, 416:238-246, 2002.

[10] Nielsen y Chuang. *Quantum Computation and Quantum Information*. Cambridge, 2000.

[11] N.A. Peters, T.C. Wei, y P.G. Kwiat. Mixed state sensitivity of several quantum information benchmarks. *Physical Review A*, 70:052309, 2004.

[12] Lieven M. K. Vandersypen, Matthias Steffen, Gregory Breyta, Costantino S. Yannoni, Mark H. Sherwood y Isaac L. Chuang. Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance. *Nature*, 414:883, 2001.

De la búsqueda de funciones booleanas con buenas propiedades criptográficas

SE PRESENTA UNA DESCRIPCIÓN GENERAL DE LAS TÉCNICAS COMPUTACIONALES Y PRINCIPIOS MATEMÁTICOS MODERNOS QUE SE UTILIZAN EN EL PROBLEMA DE BÚSQUEDA DE FUNCIONES BOOLEANAS CON MUY ALTA NO LINEALIDAD, Y OTRAS PROPIEDADES CRIPTOGRÁFICAS NECESARIAS PARA SU APLICACIÓN EN LA CRIPTOGRAFÍA DE LLAVE SIMÉTRICA.

Francisco Rodríguez Henríquez

Introducción

Las cajas de substitución (cajas *S*) constituyen la piedra angular en criptografía para lograr que los cifradores por bloque exhiban la ineludible propiedad de no linealidad.[1] En efecto, si la o las cajas *S* de un determinado cifrador por bloque no alcanzan una alta no linealidad, entonces se considera que tal algoritmo no podrá ofrecer una seguridad adecuada para impedir que información confidencial pueda ser develada por entidades no autorizadas [27,31].

Formalmente, una caja *S* es una función o correspondencia de n bits de entrada a m bits de salida, $S : Z_2^n \rightarrow Z_2^m$, esto es, una caja *S* puede ser vista como una función booleana de n bits de entrada y m bits de salida. Cuando $n = m$ la función es reversible y por lo tanto biyectiva. Sin embargo, en muchas ocasiones las cajas *S* de los cifradores por bloque no son biyectivas. Por ejemplo, como se describe en la siguiente sección, el estándar de cifrado de datos (DES, por sus siglas en inglés) emplea cajas *S* en las cuales el número de bits de entrada (seis) es mayor que el número de bits de salida (cuatro). Dada su definición, es claro que el número de funciones booleanas elegibles para diseñar una caja *S* de n bits de entrada y m bits de salida está dado por 2^{m2^n}, de tal manera que aun para valores moderados de n y m el tamaño del espacio de búsqueda de este problema tiene un tamaño desmesurado (por ejemplo, para el algoritmo DES, el total de funciones booleanas candidatas es un número con 78 dígitos decimales).

Sin embargo, no todas las funciones booleanas son apropiadas para construir buenas cajas *S*. Además de la ya mencionada propiedad de no linealidad, algunas de las principales propiedades criptográficas requeridas para dichas funciones booleanas incluyen: balance, alto grado algebraico, criterio de avalancha estricto, orden de inmunidad, etcétera.[2]

En general, los métodos para diseñar y construir funciones booleanas y cajas *S* pueden ser categorizados en tres tipos de técnicas: generación aleatoria, construcción algebraica y diseños

FRANCISCO RODRÍGUEZ HENRÍQUEZ Obtuvo el grado de doctor en 2000 en el Departamento de Ingeniería Eléctrica y Computación de la Universidad Oregon State (EUA). A partir de 2002 es profesor titular del Departamento de Computación del **Cinvestav** en la Ciudad de México. En la categoría de *Researcher & Cryptographic Designer Architect*, ha trabajado en conocidas compañías de tecnología de la información de Estados Unidos y Alemania. Sus artículos y estudios se encuentran en libros (*Cryptographic Algorithms on Reconfigurable Hardware*; Springer, 2007), revistas (*IEEE Transactions on Computers*, *IEEE Transactions on VLSI Systems* e *IEEE Transactions on Dependable and Secure Computation*) y memorias de congresos. Ha fungido como revisor técnico para más de diez revistas internacionales. Dentro de su grupo de investigación, el doctor ha desarrollado una variedad de núcleos que implementan algoritmos criptográficos relevantes y algoritmos de aritmética de campo finito en plataformas de *hardware* reconfigurable.
francisco@cs.cinvestav.mx

heurísticos [12]. El método de generación aleatoria evita con facilidad una variedad de propiedades combinatorias que son consideradas debilidades criptográficas. Sin embargo, las funciones booleanas generadas por este método no suelen exhibir buenas propiedades de no linealidad. En contraste, las construcciones algebraicas pueden brindar propiedades combinatorias específicas y una muy alta no linealidad, no obstante, tienden a tener pobre calidad en aquellas características que no fueron específicamente consideradas durante su diseño [1,9,11,30,34-35].

Una tercera estrategia para diseñar funciones booleanas y cajas *S* se basa en diseños heurísticos [2-5,10,16-17]. En este apartado, las técnicas evolutivas han sido particularmente útiles debido, especialmente, a su muy alto poder exploratorio, que les permite evaluar, a partir de una población de soluciones potenciales, vastas regiones del espacio de diseño sin necesidad de agotar exhaustivamente todo el universo de posibilidades [12]. Entre los principales logros obtenidos en el problema del diseño eficiente de cajas *S* por parte de las heurísticas evolutivas se cuentan: hallazgo de funciones booleanas con hasta nueve entradas de máxima no linealidad, confirmación/refutación de conjeturas sobre la máxima no linealidad alcanzable con funciones no lineales de siete, ocho, nueve y diez entradas, etcétera [2-5,10,16-17,22-23,28].

En este artículo se explican las aplicaciones de las cajas *S* en la llamada criptografía de llave secreta o simétrica, se describen los principios matemáticos básicos que están detrás del diseño de funciones booleanas con buenas propiedades criptográficas, y se explican varios métodos de búsqueda de dichas funciones basados en técnicas heurísticas. Finalmente, se presentan algunos de los retos y conjeturas relacionados con este ilustre problema combinatorio que, a pesar de décadas de intenso estudio, continúan abiertos.

El resto de este manuscrito está organizado como sigue. En la sección 2 se describen las aplicaciones, modos de uso y criterios de diseño que se utilizan en las cajas *S* de cifradores por bloque. En la sección 3 se definen las distintas representaciones de las funciones booleanas junto con el espectro de Walsh-Hadamard, que es una herramienta crucial para hacer la clasificación de tales funciones. Asimismo, se enlistan las principales propiedades matemáticas que deben exhibir las funciones booleanas al ser utilizadas como constructores de cajas *S*. Enseguida, en la sección 4, se esboza una metodología que mediante el uso de motores de búsqueda de heurística evolutiva permite hallar funciones booleanas con buenas propiedades criptográficas. En la sección 5 se hace un resumen, se dan algunas conclusiones y perspectivas del material cubierto en este manuscrito y se señalan algunos de los retos y problemas abiertos que han sido estudiados recientemente en la literatura abierta.

Uso de las cajas *S* en la criptografía de llave simétrica

Las técnicas científicas para la implementación de la seguridad computacional son desarrolladas por la criptografía, la cual puede sucintamente ser definida como el estudio del problema de cómo establecer un intercambio de información seguro a través del uso de un canal de comunicación que no lo es.

De manera general, los métodos de cifrado/descifrado pueden clasificarse en dos categorías: criptografía de llave simétrica y criptografía de llave pública. En el resto de esta sección se describen los aspectos de diseño más destacados de la primera clase.

La figura 1 muestra esquemáticamente el proceso de cifrado y descifrado llevado a cabo en un sistema simétrico. En los algoritmos de llave simétrica (o secreta) se presupone que cada una de las partes legítimamente involucradas en la comunicación son las únicas entidades que tienen conocimiento de la llave empleada en el proceso de cifrado/descifrado. El conocimiento de esta llave permite el descifrado del texto, de ahí la razón de que ésta deba permanecer en el más estricto secreto.

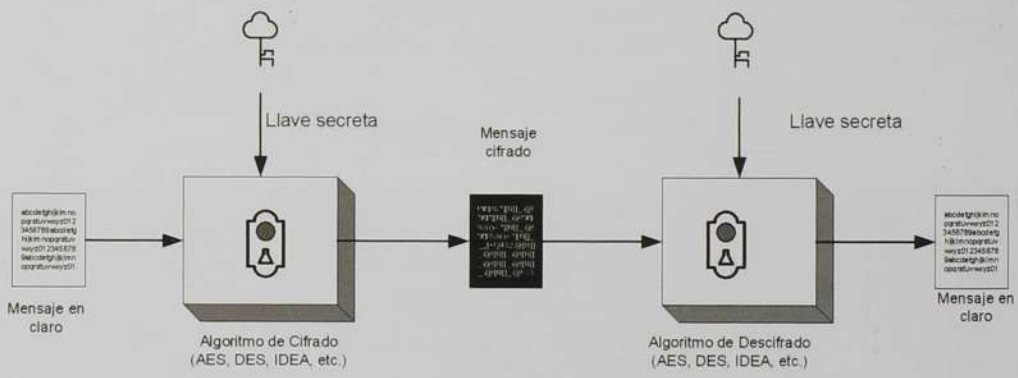


Figura 1. El proceso de cifrado y descifrado en un sistema simétrico.

Los cifradores por bloque, una subclase importante de algoritmos de llave simétrica, ofrecen diversos grados de seguridad, determinados por el tamaño en bits de la llave secreta y la calidad criptográfica en el diseño de cada cifrador. Los diseños más importantes siguen el modelo de Feistel, que por su simplicidad, buenas propiedades criptográficas y una robustez inherente, probadas a lo largo de treinta años, ha adquirido un enorme prestigio.

En la terminología criptográfica al mensaje a ser cifrado se le conoce como *texto en claro*; al proceso de codificación al que se somete al mensaje para que no pueda ser develado por entidades no autorizadas se le llama *cifrado*; al documento que resulta de cifrar el mensaje se le conoce como *criptograma*; al proceso de recuperar el mensaje en claro a partir del criptograma se le llama *descifrado* [27]. Finalmente, el término *llave* o *clave* se refiere a un valor numérico utilizado para alterar información haciéndola segura y visible únicamente a los individuos que tienen la llave correspondiente para recuperar dicha información [21].

Formalmente un *criptosistema* puede ser definido como una quíntupla $\{P,C,K,E,D\}$, donde [7]:

- P es el conjunto finito de los posibles textos en claro.
- C es el conjunto finito de los posibles textos cifrados.
- K el espacio de llaves, es un conjunto finito de todas las llaves posibles.

$\forall k \in K \exists E_k \in E$ (regla de cifrado)

$\exists D_k \in D$ (regla de descifrado)

- Cada $E_k : P \rightarrow C$ y $D_k : C \rightarrow P$ son funciones tales que

$\forall x \in P, D_k(E_k(x)) = x$

Una subclase importante de algoritmos de llave simétrica está conformada por los cifradores simétricos por bloque, que se caracterizan por dividir el texto en claro a ser cifrado en bloques de longitud fija, los cuales pueden ser o no procesados de forma independiente de acuerdo con el modo de operación en que el cifrador por bloque sea utilizado.[3]

Algunos ejemplos famosos de cifradores por bloque son: el venerable estándar de cifrado de datos (DES), adoptado en el lejano año de 1974 [8,27,31], y su sucesor, el estándar avanzado de encriptación (AES), escogido en octubre de 2000 por el Instituto Nacional de Estándares y Tecnología (NIST,[4] por sus siglas en inglés) como el estándar oficial en Estados Unidos para cifrar/descifrar documentos [20,24,26]. La principal ventaja de este tipo de esquemas es la sencillez matemática y consecuente eficiencia computacional de sus algoritmos, y su principal debilidad, el manejo y distribución de las llaves secretas entre las partes interesadas.[5] Los tamaños de las llaves utilizadas para cifrar/descifrar varían desde los 64 bits (aun cuando hoy en día se necesitan al menos 80 bits para ser consideradas realmente seguras) hasta 256 bits [24,27,31].

En el caso del estándar DES, se utiliza una longitud de llave de apenas 56 bits. A pesar que en el tiempo de su creación esta longitud de llave fue considerada muy segura, los avances tecnológicos han permitido el desarrollo de técnicas para encontrar las llaves por búsqueda exhaustiva en tiempos relativamente cortos. Por ejemplo, ya desde 1999 un proyecto de cómputo distribuido *rompió* DES en un tiempo de 22 horas con 15 minutos. Debido a ello, desde hace mucho tiempo DES no es considerado suficientemente robusto para aplicaciones de alta seguridad, por lo que en la práctica profesional se utiliza una variante conocida como *triple DES*, la cual brinda una seguridad equivalente a la proporcionada por una llave de 112 bits [27].

Los cifradores por bloque ofrecen diversos grados de seguridad, determinados esencialmente por el ya mencionado tamaño en bits de la llave secreta y por la propia calidad criptográfica en el diseño de cada cifrador. Hoy en día, muchos de los diseños más importantes de cifradores por bloque siguen el modelo de Feistel. Ello se debe a que este modelo se caracteriza por su simplicidad, buenas propiedades criptográficas y una robustez inherente. Por otro lado, los cifradores por bloque de Feistel han adquirido un enorme prestigio tras resistir exitosamente el escrutinio exhaustivo que sobre ellos ha realizado la comunidad criptográfica de manera implacable a lo largo de los últimos treinta años [31].

Los cifradores de Feistel utilizan transformaciones lineales en forma de corrimientos lógicos, operadores booleanos a nivel bit, etcétera, y transformaciones no lineales que son implementadas con bloques de substitución de bits, conocidos en la literatura especializada como cajas S. Dado que las cajas S son los únicos bloques no lineales presentes en el modelo de Feistel, se acepta de manera general que la calidad en eficiencia y seguridad de un algoritmo cifrador depende en buena medida del buen diseño de dichos módulos.

Por ejemplo, en el caso del cifrador DES están definidas un total de 8 cajas *S*. Cada una de estas cajas puede ser representada como una tabla con 64 casillas dispuestas en 4 renglones y 16 columnas [27,31]. El proceso de substitución de un valor de entrada de 6 bits por uno de salida de 4 bits[6] opera de la siguiente manera:

Dado el dato de entrada, $a_0a_1a_2a_3a_4a_5$, el primer y último bit, esto es, a_0a_5, representan el número de renglón, mientras que los 4 bits restantes, esto es, $a_1a_2a_3a_4$, representan el número de columna. Así, cualquiera de las 8 cajas *S* de DES substituirá *A*=101011 con el valor almacenado en el cuarto renglón (11) y la sexta casilla (0101). Por ejemplo, si al dato *A* se le aplica la caja de substitución S_3 (véase figura 2), el valor substituido será 1001 (9). Si en cambio el mismo dato *A* es substituido utilizando la caja S_7, el resultado de la substitución será 0100 (4).

Como se muestra en la figura 2, todos los renglones de todas las cajas *S* de DES son permutaciones de los dieciséis números enteros que pueden representarse con 4 bits, esto es: 0,1,...,15. Además, los valores contenidos en las cajas *S* fueron diseñados así que si se tienen dos datos de entrada que difieren por un solo bit, las correspondientes salidas diferirán por al menos dos bits.[7]

Resulta interesante señalar que aunque los criterios completos de diseño de las cajas *S* de DES no han sido nunca desclasificados, la perspectiva que dan más de treinta años de criptoanálisis permite tener hoy la casi certeza que sutiles debilidades fueron introducidas a propósito en las propiedades

Renglón	Columnas																Cajas S
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7	S1
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8	
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0	
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13	
0	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10	S2
1	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5	
2	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15	
3	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9	
0	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8	S3
1	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1	
2	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7	
3	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12	
0	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15	S4
1	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9	
2	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4	
3	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14	
0	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9	S5
1	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6	
2	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14	
3	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3	
0	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11	S6
1	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8	
2	9	14	15	5	2	8	12	3	7	0	14	10	1	13	11	6	
3	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13	
0	4	11	2	14	15	0	8	13	3	2	9	7	5	10	6	1	S7
1	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6	
2	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2	
3	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12	
0	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7	S8
1	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2	
2	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8	
3	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11	

Figura 2. Formación de los renglones de las cajas *S* de DES.

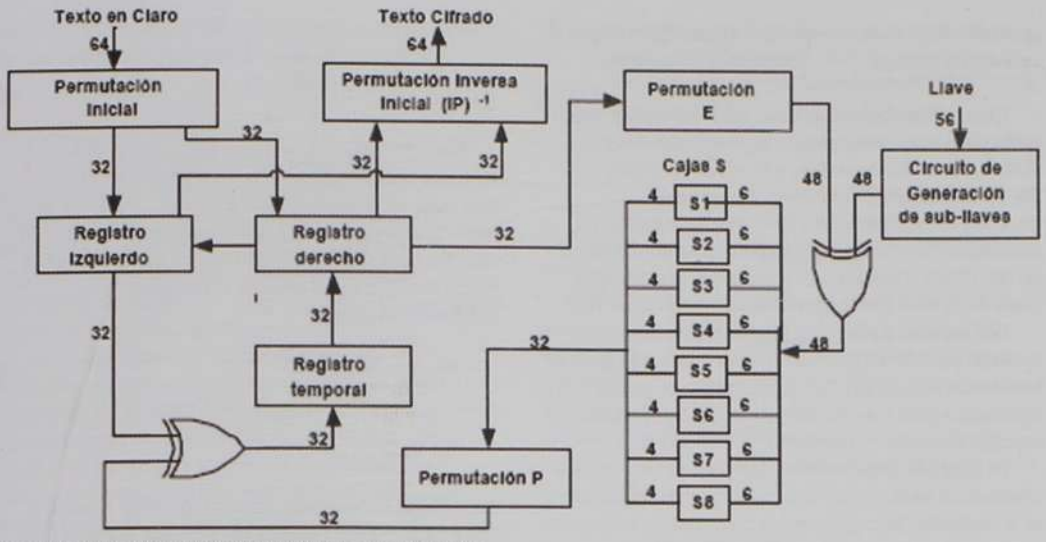


Figura 3. Diversas transformaciones de un bloque de texto en claro.

no lineales de las cajas *S*, debilidades que hicieron a DES vulnerable al criptoanálisis diferencial y lineal inventados en los años noventa [31].[8]

La figura 3 muestra las diversas transformaciones que un bloque de texto en claro de 64 bits sufre en la iteración principal del algoritmo DES. Se puede apreciar en el extremo derecho inferior de dicha figura que las 8 cajas *S* se encargan de procesar en paralelo 48 bits de entrada produciendo una salida de 32 bits. En una implementación en hardware, cada una de las 8 cajas *S* de DES utiliza un espacio de memoria de $64 \times 4 = 256$ bits, por lo que se necesitan 2K bits de memoria para almacenar las 8 cajas *S* a la manera descrita en la figura 2.

Como se mencionó en la introducción, para que las cajas *S* puedan ser consideradas útiles en aplicaciones criptográficas deben cumplir ciertas propiedades tales como una alta no linealidad, un alto grado algebraico, un alto orden de inmunidad de correlación y una baja autocorrelación, entre otras. Para describir estas propiedades de una manera formal, en la siguiente sección se revisan las definiciones matemáticas más relevantes a este problema.

Definiciones matemáticas básicas

Una caja *S* de *n* bits × *m* bits es una relación tal que $S : Z_2^n \rightarrow Z_2^m$. Así, una caja *S* puede ser representada como 2^n números de *m* bits, denotados por $r_0, \ldots, r_{2^n-1}$, en donde $S(x) = r_x, 0 \leq x \leq 2^n$ y donde r_x representa los renglones de la caja *S*. Alternativamente, una caja *S* puede también representarse mediante una matriz binaria *M* de $2^n \times m$ bits, donde la entrada *i, j* es el bit *j* del renglón *i*-ésimo.

En la práctica, resulta suficiente estudiar cajas *S* de *n* variables de entrada con un solo bit de salida,[9] a las que llamaremos, por simplicidad, funciones booleanas de *n* variables, y las cuales serán el objeto de estudio en el resto de esta sección.

Una función booleana de *n* variables, $f(x) : Z_2^n \rightarrow Z_2$, es entonces una relación de *n* entradas binarias a una sola salida binaria. Llamaremos B_n al conjunto de las 2^{2^n} funciones booleanas de *n* variables. La representación básica de una función booleana es su *tabla de verdad*, la cual consiste en una cadena binaria de longitud 2^n, tal que:

$$f = \left[f(0,\ldots 0,0), f(0,\ldots 0,1), \ldots, f(1,\ldots 1,1) \right] \qquad (1)$$

Es importante remarcar que por simplicidad, en muchas ocasiones la cadena binaria en (1) se escribe utilizando su correspondiente representación hexadecimal.

El peso de Hamming de una cadena *S* es el número de unos en *S* y se denota como *H*(*S*). Se dice que una función booleana de *n*-variables está balanceada si su tabla de verdad contiene un número

Las técnicas científicas para la implementación de la seguridad computacional son desarrolladas por la criptografía, disciplina que estudia el problema de cómo establecer un intercambio de información seguro, a través del uso de un canal de comunicación que carece de esa seguridad.

igual de ceros y unos, esto es, si acaso $H(f) = 2^{n-1}$. En B_n, existen un total de $\binom{2^n}{2^{n-1}}$ funciones balanceadas.

Como se mencionó arriba, las 2^n salidas de una tabla de verdad tradicional están definidas sobre Z_2, esto es, sus salidas pueden tomar los valores $\{0, 1\}$. Sin embargo, notando que el grupo $\{0, 1, \oplus\}$ es isomórfico a $\{1,-1, *\}$, resulta útil considerar funciones booleanas con símbolos de salida $\{1, -1\}$. Llamaremos a esa representación la tabla de verdad polar de la función booleana $\hat{f}(x)$.

Por razones históricas, la representación polar se prefiere para la mayoría de los cálculos en funciones booleanas [5,9,22-23]. Tal representación puede ser obtenida a partir de la tabla de verdad de f usando la sencilla fórmula $\hat{f}(x) = (-1)^{f(x)} = 1 - 2f(x)$.

La llamada *forma normal algebraica* es una tercera alternativa para representar una función booleana de n variables, la cual consiste en expresar la función booleana como un polinomio multi-variable a través de la suma XOR[10] mínima de productos AND, es decir, dado $S = \{1, 2, \ldots, n\}$,

$$f(x_1,\ldots,x_n) = a_0 \oplus a_1x_1 \ldots \oplus a_nx_n \oplus a_{12}x_1x_2 \ldots \oplus a_{n-1,n}x_{n-1}x_n \ldots \oplus a_{12\ldots n}x_1x_2\ldots x_n = \bigoplus_{\omega} a_\omega \prod_{i\in\omega} x_i \quad (2)$$

Se dice que una función booleana L_ω es *lineal* si puede ser definida como la suma XOR de productos AND de un subconjunto de variables de entrada y los coeficientes de ω así que:

$$L_\omega(x) = \omega_1x_1 \oplus \omega_2x_2 \oplus \ldots \oplus \omega_nx_n \quad (3)$$

donde $n, \omega \in Z_2^n$. El conjunto de *funciones afines* está conformado por el conjunto de funciones lineales y sus complementos $A_{\omega,c}(x) = L_\omega(x) \oplus c$ con $c \in \{0,1\}$.

La *distancia de Hamming* entre dos funciones $f \in B_n$ y $g \in B_n$ está definida como el número de posiciones en la tabla de verdad en donde las funciones difieren y pueden ser expresadas como el peso de Hamming de la suma XOR de las dos funciones, esto es, $dist(f, g) = H(f \oplus g)$. Entonces, la *correlación* entre las funciones f y g está dada por:

$$c(f,g) = 1 - \frac{\text{dist}(f,g)}{2^n - 1} \quad (4)$$

Sean $x = (x_1,\ldots x_n)$ y $\omega = (\omega_1,\ldots\omega_n)$ dos vectores binarios de n bits, cuyo producto punto está definido como, $x \cdot \omega = x_1\omega_1 \oplus \ldots xn\omega_n$, y sea f una función booleana de n variables. Entonces, la transformada de Walsh-Hadamard de una función f es la función F definida en el dominio de la frecuencia ω como:

$$F(\omega) = \sum_{x\in Z_2^n} (-1)^{\hat{f}(x)\oplus x\cdot\omega} \quad (5)$$

con $\omega \in Z_2^n$.

A partir de (5) se colige que una función booleana f de n variables es balanceada si y sólo si $F(\omega) = 0$.[11] El vector $\{F(0),\ldots,F(2^n-1)\}$ es el espectro de Walsh-Hadamard de la función f, y se denota al valor absoluto del máximo coeficiente del espectro como:

$$WH_{\max}(f) = \max_{w\in Z_2^n} |F(\omega)| \quad (6)$$

Correspondientemente, la transformada inversa de Walsh-Hadamard de una función F, formulada a través de la representación polar de una cierta función $\hat{f}$ está dada por:

$$\hat{f}(x) = 2^{-n} \sum_{\omega} F(\omega)(-1)^{\omega\cdot x} \quad (7)$$

Nótese que un cálculo directo del espectro de Walsh-Hadamard completo utilizando (5) implica una complejidad de N^2 pasos, con $N=2^n$. Sin embargo, tal y como ocurre con la transformada rápida de Fourier, es posible definir un procedimiento rápido para el cálculo de la transformada de Walsh-Hadamard que puede ser computado con únicamente $N\log(N)$ pasos. Para lograr esa aceleración, la Transformada Rápida de Walsh-Hadamard (TRWH) utiliza el concepto de *diagrama de mariposa* (ver figura 4). Un diagrama de mariposa de tamaño 2 (el tamaño más

Además de lineales, los cifradores de Feistel utilizan transformaciones no lineales, que son implementadas con bloques de substitución de bits, conocidos en la literatura especializada como cajas S. Por tratarse de los únicos bloques no lineales presentes en el modelo, generalmente se acepta que la calidad en eficiencia y seguridad de un algoritmo cifrador depende, en gran parte, del buen diseño de dichos módulos.

pequeño) toma dos bits de entrada (x_0, x_1) y produce dos bits de salida (y_0, y_1) de la siguiente manera:

$$y_0 = x_0 + x_1$$
$$y_1 = x_0 - x_1 \quad (8)$$

En general, la TRWH divide recursivamente el cálculo de un vector de tamaño $n=rm$, en r transformaciones más pequeñas de tamaño m, donde r es la base de la transformación. Estas r transformaciones pequeñas son combinadas utilizando diagramas de mariposa de tamaño r, las cuales a su vez, son TRWH de tamaño r.[12]

La no linealidad de una función booleana f está definida como el número de bits que deben cambiarse en la tabla de verdad en esa función booleana para obtener la función afín más cercana (en el sentido de la distancia de Hamming) [1,3,11]. Se demuestra que la no linealidad de una función f puede calcularse directamente a partir de $|WH_{\max}(f)|$, el máximo valor absoluto en el espectro de Walsh-Hadamard a través de la siguiente expresión:

$$N(f) = \frac{1}{2}\left(2^n - |WH_{\max}(f)|\right) \quad (9)$$

La aplicación del celebrado *Teorema de Parseval* al dominio de funciones booleanas establece que la suma de los cuadrados de cada uno de los coeficientes del espectro de Walsh-Hadamard es siempre igual a 2^{2n}, esto es:

$$\sum_{\omega \in Z_2^n} \left(\hat{F}(\omega)\right)^2 = 2^{2n} \quad (10)$$

Una consecuencia inmediata de este resultado es que $WH_{\max}(f) \geq 2^{n/2}$. Basado en esta observación se definen las funciones curvas,[13] las cuales son funciones booleanas de n variables de entrada tales que,

$$\left|F(\omega) = 2^{\frac{n}{2}}\right|, \forall \omega \in 0,\ldots,2^n - 1 \quad (11)$$

Las funciones booleanas curvas sólo están definidas para un número de variables de entrada par y siempre resultan ser funciones booleanas desbalanceadas[14] de máxima no linealidad (lo cual se puede demostrar a partir de la definición (7) y el hecho que $|WH_{\max}(f)|$ toma su valor mínimo teórico: $2^{n/2}$).

Se define la *función de autocorrelación* $r_{\hat{f}}(s)$, de una función booleana f a partir de su representación polar como:

$$r_{\hat{f}}(s) = \sum_x \hat{f}(x)\hat{f}(x \oplus s) \quad (12)$$

con $s \in Z_2^n$.

Finalmente mencionaremos el teorema de Titsworth [3], que establece que F evaluado en el dominio de la frecuencia corresponde al espectro de Walsh-Hadamard de una función booleana si y sólo si:

$$\sum_{\omega \in Z_2^n} F(\omega)F(\omega \oplus s) = \begin{cases} 2^{2n} & \text{si } s = 0 \\ 0 & \text{en otro caso} \end{cases} \quad (13)$$

con $s \in Z_2^n$.

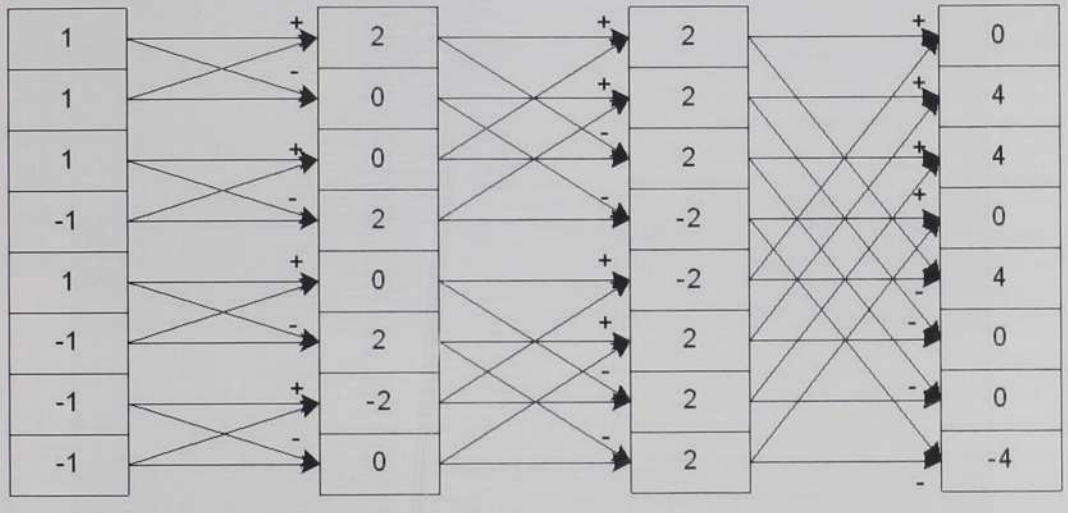


Figura 4. Diagrama de mariposa.

Ejemplos

Aquí se ilustran las definiciones dadas en la subsección precedente con varios ejemplos.

Ejemplo 1. Número de funciones balanceadas. La tabla I muestra el número de funciones booleanas balanceadas y respectivo porcentaje en el total de B_n funciones booleanas para n=1,2,...,6. Como puede apreciarse, hay una relativa abundancia de funciones balanceadas en el enorme universo de funciones booleanas B_n, que, sin embargo, decae rápidamente conforme n se incrementa.

Ejemplo 2. Función booleana de tres entradas, balanceada y de máxima no linealidad. Consideremos la función booleana f de tres entradas descrita algebraicamente como:

$$f(x)=x_2x_1+x_3x_1+x_3x_2 \quad (14)$$

La tabla II presenta la tabla de verdad de la función f en su versión tradicional y polar, junto con su respectivo espectro de Walsh-Hadamard.

El espectro de f puede ser hallado a través de la ecuación (5), o aún mejor, utilizando la Transformada Rápida de Walsh-Hadamard mostrada esquemáticamente en la figura 4.

Como se explicó en la subsección precedente, el espectro $F(\omega)$ de una función booleana f brinda una rica información sobre las características de dicha función. Por ejemplo, el espectro de Walsh-Hadamard de la tabla 2 nos indica que f es una función balanceada, puesto que el primer coeficiente del espectro, $F(0)$, tiene valor cero. Asimismo, se determina a partir de (9) que f tiene no linealidad 2 puesto que[15]:

$$N(f)=\frac{1}{2}\left(2^n-\left|WH_{\max}(f)\right|\right)=\frac{1}{2}\left(2^3-4\right)=2$$

$$f(x)=x_2x_1+x_3x_1+x_3x_2.$$

Ejemplo 3. Función curva de 4 entradas. Considere la función booleana f de cuatro entradas descrita algebraicamente como:

$$f(x)=\bar{x}_4\bar{x}_3x_2x_1+x_4x_3\left(\bar{x}_2+\bar{x}_1\right)+\bar{x}_2\bar{x}_1\left(x_3+x_4\right) \quad (15)$$

Tabla I. Número de funciones balanceadas en B_n.

N	B_n	Func. balanceadas	Porcentaje
1	2^2=4	$\binom{2^1}{2^0}=\binom{2}{1}=2$	50.0%
2	2^4=16	$\binom{2^2}{2^1}=\binom{4}{2}=6$	37.5%
3	2^8=256	$\binom{2^3}{2^2}=\binom{8}{4}=70$	27.3%
4	2^{16}=64 Kilos	$\binom{2^4}{2^3}=\binom{16}{8}=12870$	19.6%
5	2^{32}=4 Gigas	$\binom{2^5}{2^4}=\binom{32}{16}\approx 601Meg$	14.0%
6	2^{64}=16 Exas	$\binom{2^6}{2^5}=\binom{64}{32}\approx 1.6exas$	9.9%

Tabla II. Ejemplo de una función booleana de 3 entradas

x_3	x_2	x_1	$f(x)$	$\hat{f}(x)$	$F(\omega)$
0	0	0	0	1	0
0	0	1	0	1	4
0	1	0	0	1	4
0	1	1	1	-1	0
1	0	0	0	1	4
1	0	1	1	-1	0
1	1	0	1	-1	0
1	1	1	1	-1	-4

La tabla III presenta la tabla de verdad de la función *f* en su versión tradicional y polar, junto con su respectivo espectro de Walsh-Hadamard. Del espectro de Walsh-Hadamard de la tabla III podemos deducir que la función booleana *f* en (15), satisface la definición de función curva de la ecuación (11). Nótese que, como se afirmó en la subsección precedente, la tabla de verdad de *f* corresponde a la de una función booleana no balanceada con máxima no linealidad 6, puesto que:

$$N(f)=\frac{1}{2}\left(2^n-\left|WH_{\max}(f)\right|\right)=\frac{1}{2}\left(2^4-4\right)=6$$

Tabla III. Tabla de verdad de una función curva de 4 entradas

x_4	x_3	x_2	x_1	$f(x)$	$\hat{f}(x)$	$F(\omega)$
0	0	0	0	0	1	4
0	0	0	1	0	1	-4
0	0	1	0	0	1	-4
0	0	1	1	1	-1	-4
0	1	0	0	1	-1	4
0	1	0	1	0	1	4
0	1	1	0	0	1	4
0	1	1	1	0	1	-4
1	0	0	0	1	-1	-4
1	0	0	1	0	1	4
1	0	1	0	0	1	4
1	0	1	1	0	1	4
1	1	0	0	1	-1	-4
1	1	0	1	1	-1	4
1	1	1	0	1	-1	4
1	1	1	1	0	1	4

Propiedades criptográficas deseables en funciones booleanas

A continuación se enlistan varios de los principales criterios utilizados en la práctica profesional para diseñar cajas *S* con buenas propiedades criptográficas:

1. Balance. Esta propiedad es muy deseable para evitar ataques cripto-diferenciales tales como los introducidos por A. Shamir contra el algoritmo DES [27,31-33].

2. Alta no linealidad. Esta propiedad reduce el efecto de los ataques por criptoanálisis lineal. Como se discutió antes, la no linealidad de una función booleana puede ser calculada directamente de la transformada de Walsh-Hadamard (a través de la ecuación (5)).

3. Autocorrelación. Este valor es proporcional al desbalance de todas las derivadas de primer orden de la función booleana. Valores pequeños son considerados como buenos mientras que un valor grande es considerado un símbolo de debilidad. Las funciones curvas, estudiadas en la subsección precedente, gozan de una autocorrelación mínima, por lo que optimizan esta propiedad.

4. Indicador absoluto. Indicador absoluto de una función booleana denotado por *M(f)* está dado por $|r_{max}|$ el máximo valor absoluto en $r_f(s)$ (véase (12)). Se considera que una función booleana con un *M(f)* pequeño es criptográficamente deseable. Nuevamente, las funciones curvas tienen una autocorrelación óptima, pues su indicador absoluto es cero [1,3,11].

5. Efecto avalancha. Está relacionado con la autocorrelación y se define con respecto a un bit específico de entrada tal que al complementarlo resulta en un cambio en el bit de salida con una probabilidad de 1/2. El criterio de avalancha estricto (SAC por sus siglas en inglés),[16] requiere los efectos avalancha de todos los bits de entrada. Se dice que una función booleana satisface el criterio de avalancha estricto si al complementar un solo bit de entrada resulta en un cambio en un bit de salida con una probabilidad de 1/2. Puede demostrarse fácilmente que una función booleana *f* con función de autocorrelación $r_f(s)$, satisface el criterio de avalancha estricto si y sólo si $r_f(s)=0$ para toda *s* con peso de Hamming *H(s)*=1 [13-14].

Para diseñar cajas *S* con buenas propiedades criptográficas es necesario seguir criterios que contemplan propiedades tales como balance, alta no linealidad, autocorrelación, indicador absoluto, efecto avalancha, grado algebraico, orden de inmunidad de correlación y resistencia.

6. Grado algebraico. El grado algebraico de una función f, denotado como $deg(f)$, es el número de entradas más grande que aparece en cualquier producto de la forma normal algebraica. Esto es, $x_1 \oplus x_2$ tiene grado 1 (es decir, es lineal) mientras que $x_1 \oplus x_1 x_2 x_3$ tiene grado 3 [3,16-17].

7. Orden de inmunidad de correlación. Una función f tiene un orden de inmunidad de correlación m si y sólo si [9]:

$$\hat{F}(\omega) = 0; 1 \leq H(\omega) \leq m$$

8. Resistencia. Una función f que tiene inmunidad de correlación de orden m, es *resistente* si y sólo si también es balanceada [9]:

$$\hat{F}(\omega) = 0; 0 \leq H(\omega) \leq m$$

Discusión de compromisos y conflictos en las propiedades de las cajas S

De manera ingenua, uno podría plantearse buscar funciones booleanas que reúnan todas las propiedades criptográficas descritas en la subsección anterior. Así, podría ensayarse el vano intento de hallar funciones booleanas balanceadas, con máxima no linealidad, alto grado algebraico, alto orden de inmunidad de correlación y baja autocorrelación.

Sin embargo, es *imposible* que alguna función booleana pueda satisfacer al mismo tiempo todos esos criterios.

Quizás el ejemplo más socorrido para ilustrar esa realidad son las funciones curvas, las cuales por definición (véase ecuación (9)) son máximamente no lineales *pero* desbalanceadas. Si desistimos de las funciones curvas y nos concentramos en funciones balanceadas (esto es $F(0)=0$), entonces, y como consecuencia del teorema de Parseval de la ecuación (10), algún otro coeficiente del espectro deberá necesariamente compensar ese faltante teniendo una magnitud mayor que $2^{n/2}$, lo cual reducirá la no linealidad de esa función. Otro conflicto más ocurre al intentar maximizar el orden de inmunidad, lo cual sólo puede llevarse a cabo en detrimento de la no linealidad [3]. Se conocen funciones booleanas curvas que exhiben máxima no linealidad y sin embargo tienen bajísimos grados algebraicos. Por otro lado, es posible hallar funciones con baja no linealidad pero con alto grado algebraico [1].

Debido a los conflictos existentes en las propiedades deseables para una función booleana, es necesario establecer compromisos. De esa manera, se ha ido adoptando más y más en la literatura especializada [1,3-5,16-17] el perfil de una función booleana f balanceada, dado por la cuádrupla (n, m, d, nl), donde n denota el número de variables de entrada, m el orden de inmunidad, d el orden algebraico y nl la no linealidad de la función f.[17]

Búsqueda de funciones booleanas por métodos heurísticos

Para poder realizar una búsqueda basada en técnicas heurísticas evolutivas, es indispensable contar con una *representación* que permita codificar las soluciones potenciales del problema en una población inicial de *individuos*. En seguida es necesario definir operadores que, generación tras generación, alteren las características de los individuos, así que en cada generación, a los individuos con mejores características se les dé una mayor oportunidad de reproducirse, mejorando sus oportunidades de sobrevivir.

Los operadores que típicamente se utilizan en este tipo de heurísticas son la *mutación*, la *selección* y la *cruza*. En particular, para poder implementar el mecanismo de *selección*, resulta indispensable contar con una función de *aptitud* que permita medir el desempeño de la solución representada en cada uno de los individuos de la población bajo análisis [13-15,19].

En el caso de una búsqueda heurística de funciones booleanas, el problema de diseño más importante es decidir cuál será la función de aptitud que se utilizará para medir las bondades criptográficas de los individuos (funciones booleanas) que constituyen la población de cada generación [4-5,13]. En los últimos años se han propuesto diversas funciones de aptitud, de las cuales, en el resto de esta sección, se discutirán las siguientes tres: las tradicionales, las que se basan en inversión de espectro y en espacios restringidos.

Funciones de aptitud tradicionales

La abrumadora mayoría de los trabajos reportados antes del año 2000 [16-17] enfilaban todos los cañones hacia la búsqueda de funciones altamente no lineales, sin reparar, ni poco ni mucho, en otras propiedades criptográficas. Así se propuso la medida de no linealidad de un individuo dado (esto es, alguna función booleana f) como su medida de aptitud:

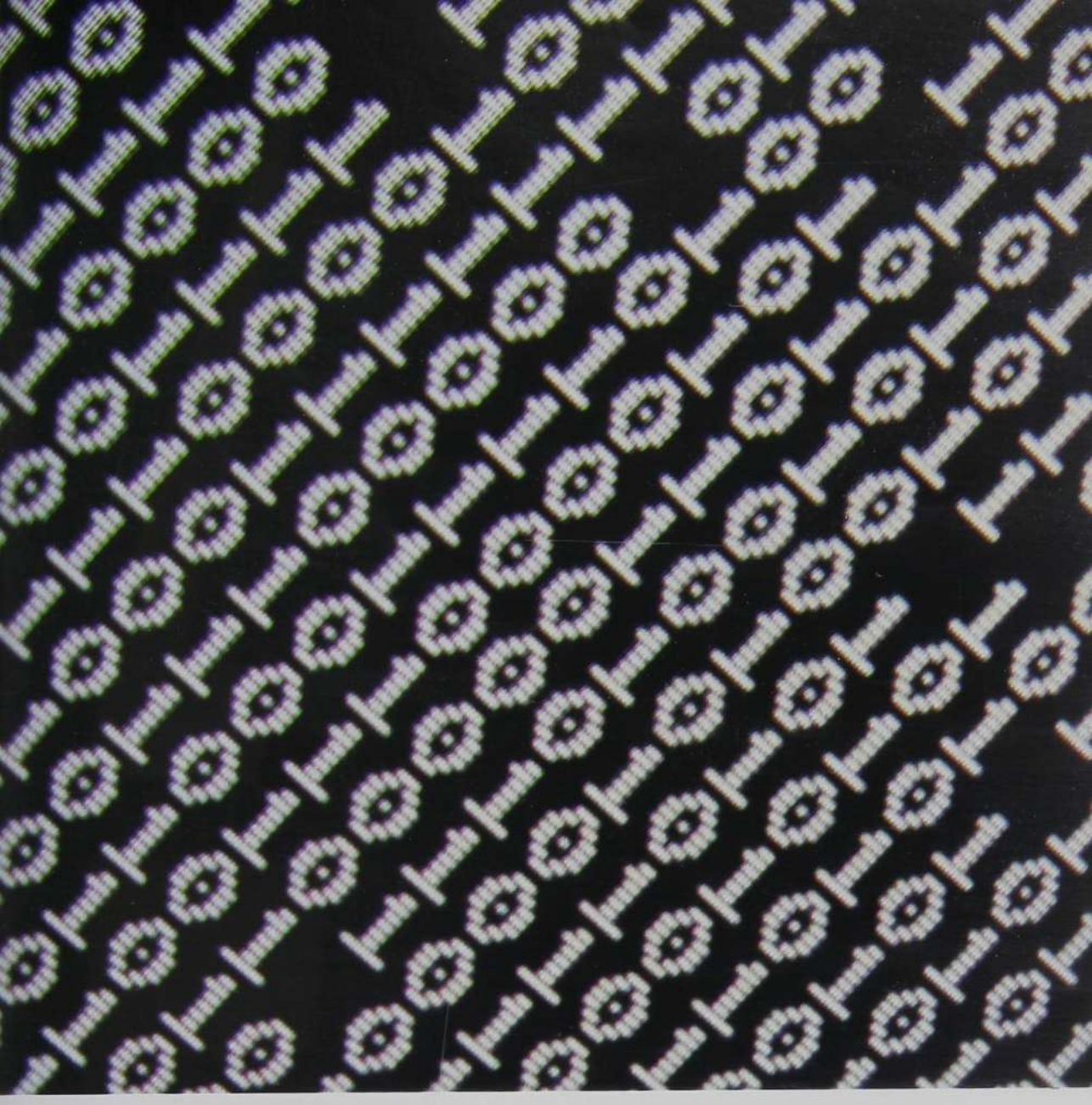
$$Aptitud(f) = \frac{1}{2}\left(2^n - \left|WH_{\max}(f)\right|\right)$$

o visto como un problema de minimización, la función de aptitud se planteó también como:

$$costo(f) = \left|WH_{\max}(f)\right| = \max_{\omega}\left|\hat{F}(\omega)\right|$$

De manera similar, en los raros casos en que se fijó la baja autocorrelación como función objetivo, se utilizó una función de costo dada por:

$$costo(f) = AC(f) = \max_{s \neq 0}\left|\sum_{x} \hat{f}(x)\hat{f}(x \oplus s)\right| = \max_{s \neq 0}\left|\hat{r}(s)\right| \text{ con } s \in Z_2^n$$



Para realizar una búsqueda en técnicas heurísticas evolutivas, los operadores que típicamente se utilizan son la mutación, la selección y la cruza.

Funciones de aptitud basadas en inversión de espectro

Como se ha mencionado anteriormente, el espectro de Walsh-Hadamard de una función booleana f permite evaluar rápidamente si los diferentes criterios de diseño han sido alcanzados o no. Es por ello que en años recientes se propuso desarrollar motores de búsqueda basados en las características que el espectro debiera tener en una buena función booleana. Esta estrategia realiza entonces una suerte de "ingeniería en reversa", en el sentido que la búsqueda se enfoca primero en diseñar el espectro con las características que se desean, para después, a través de la aplicación de la transformada inversa de Walsh-Hadamard, hallar la función booleana a la que le corresponde tal espectro.

En concreto, supongamos que se cuenta con el espectro de Walsh-Hadamard $F(\omega)=\{F(0), F(1),..., F(2^n-1)\}$, de una función con perfil criptográfico (n, m, d, nl), esto es, el espectro correspondiente al de una función booleana balanceada de n variables de entrada con no linealidad nl, grado algebraico d y orden de inmunidad m.[18] Consideremos entonces el conjunto de espectros P dado por todas las posibles permutaciones del espectro original $F(\omega)$ tales que $P(\omega)=0; 0 \le H(\omega) \le m$. Entonces cualquier espectro G incluido en el conjunto P disfruta de los mismos valores y propiedades criptográficos con los que cuenta el espectro original F.

Desafortunadamente, esta estrategia no garantiza que un espectro permutado G en el conjunto P corresponderá a alguna función booleana legítima. En efecto, cuando se aplica la transformada inversa a G:

$$\hat{p}(x)=2^{-n}\sum_{\omega} G(\omega)(-1)^{\omega x} \quad ,$$

la función resultante $\hat{p}$ tendrá, en general, coeficientes reales, en vez de tener todos sus coeficientes en $\{1,-1\}$, como corresponde a la representación polar de toda verdadera función booleana. Debido a ello, en [3] se propuso utilizar una asignación heurística para evaluar la *desviación* del espectro G a un espectro legítimo. Se define la función booleana $\hat{b}$ así que:[19]

$$\hat{b}(x)=\begin{cases} +1 & \text{si } \hat{p}(x)>0 \\ -1 & \text{si } \hat{p}(x)<0 \\ +1 \text{ o } -1 & \text{si } \hat{p}(x)=0 \end{cases}$$

Con lo que de manera natural surge como función de costo la ecuación que mide cuán lejos quedó la permutación espectral G de una verdadera función booleana, es decir [3]:

$$Costo(G)=\sum_{x=0}^{2^n-1}\left(\hat{p}(x)-\hat{b}(x)\right)^2 \qquad (16)$$

La función de costo en (16) tiene el defecto de hacer las evaluaciones en el dominio booleano abandonando el dominio de la frecuencia ω donde está definida la permutación espectral G. Es por ello que en [3] se definió una función de costo en el dominio de la frecuencia, fundamentada en el teorema de Titsworth, enunciado en la sección precedente (véase la ecuación (13)):

$$\cos to(G)=\sum_{s}\left(\left|\sum_{\omega\in Z_2^n} G(\omega)G(\omega\oplus s)\right|\right)-2^{2n}=0 \qquad (17)$$

con $s \in Z_2^n$.

Utilizando la función de costo (17) se hicieron en [6] experimentos para hallar funciones booleanas con perfil criptográfico (7, 0, 6, 56), correspondiente a una función booleana de siete variables de entrada, balanceada, con orden de inmunidad 0, grado algebraico 6 y no linealidad 56.[20] Se utilizó un algoritmo genético simple con porcentaje de mutación en el rango de [1/100, 1/128] y porcentaje de cruza 0.7, obteniéndose resultados favorables en todas las corridas. Por ejemplo, una de las funciones halladas en [6] que satisface el perfil buscado es:

6A65 33AC D05E C840 07BA 4597 BD81 BE7B

Asimismo, en [6] se encontró la siguiente función booleana que satisface el perfil criptográfico (7,2,4,56):

039CE9F8D781253EA6555E4A22E8F11F

En el caso de una búsqueda heurística de funciones booleanas, el problema de diseño más importante es decidir cuál será la función de aptitud que se utilizará para medir las bondades criptográficas de los individuos (funciones booleanas) que constituyen la población de cada generación; si las tradicionales o las que se basan en inversión de espectro y en espacios restringidos.

Tabla IV. Número de funciones booleanas de rotación simétrica en B_n

	2	3	4	5	6	7	8	9
B_n	2^4	2^8	2^{16}	2^{32}	2^{64}	2^{128}	2^{256}	2^{512}
FBRS	2^3	2^4	2^6	2^8	2^{14}	$\approx 2^{19}$	$\approx 2^{32}$	$\approx 2^{57}$

Búsquedas en espacios restringidos

Aunque el método de búsqueda por inversión espectral ha dado en los últimos tres años excelentes resultados [3-5], sigue estando limitado por el hecho que el espacio de búsqueda B_n tiene un crecimiento doblemente exponencial con n. Por ello, en trabajos más recientes [16-17,28] se ha utilizado un refinamiento del método de búsqueda por inversión espectral restringiendo el espacio de búsqueda al asociado a las funciones booleanas de rotación simétrica (FBRS).[21]

Las FBRS son funciones booleanas que mantienen el mismo valor para todas las rotaciones cíclicas de sus entradas. Por ejemplo, para una FBRS de 5 variables de entrada se definen las siguientes 8 clases u *órbitas* [3,16-17,25,34-35] de rotación:

Órbita 1: $f(00000)$
Órbita 2: $f(00001)=f(00010)=f(00100)=f(01000)=f(10000)$
Órbita 3: $f(00011)=f(00110)=f(01100)=f(11000)=f(10001)$
Órbita 4: $f(00101)=f(01010)=f(10100)=f(01001)=f(10010)$
Órbita 5: $f(01011)=f(10110)=f(01101)=f(11010)=f(10101)$
Órbita 6: $f(00111)=f(01110)=f(11100)=f(11001)=f(10011)$
Órbita 7: $f(01111)=f(11110)=f(11101)=f(11011)=f(10111)$
Órbita 8: $f(11111)$

La tabla IV muestra el número de funciones booleanas de rotación simétrica en el universo total de B_n funciones booleanas para n=2,3,...,9.

Una propiedad muy útil de las FBRS es que el espectro de Walsh-Hadamard toma el mismo valor para todos los elementos que pertenezcan a la misma órbita [28]. Además, a pesar de que el conjunto de FBRS representa sólo una pequeña fracción de todas las posibles funciones booleanas, el conjunto de funciones FBRS tiende a tener una muy rica no linealidad [16-17].

Utilizando una búsqueda heurística del máximo gradiente restringida al subespacio de las funciones FBRS y empleando la técnica de inversión espectral, se reportó en diciembre de 2006 la siguiente función booleana de nueve variables con no linealidad 241 [17]:

977F 3FFA 0EFA AEC9 55F8 FACD CCA9 A083 7666
EBC0 FA88 E0B3 F4E0 8983 C845 915E 7F7C 2C29
FCCB A101 EA98 C085 E811 8B5E FE21 E911 8483
851E E195 2136 9716 76E9

En importante señalar que desde 1974 se había conjeturado que tal función podría existir, pero tuvieron que pasar más de 30 años para poder confirmar esa afirmación con evidencia experimental [17].

De conjeturas, retos y perspectivas

La ecuación (11) de la sección 3, define a las funciones curvas, las cuales se caracterizan por alcanzar una no linealidad máxima (con valor de $2^{n-1}-2^{n/2-1}$), para funciones booleanas de n variables con n par. Sin embargo, como se ha mencionado, las funciones curvas son siempre desbalanceadas, por lo que cabe preguntarse:

¿Cuál es la máxima no linealidad alcanzable por una función booleana balanceada de n variables, con n par?

Hasta diciembre del año pasado sólo se conocían ejemplos de funciones booleanas con valores de no linealidad $2^{n-1}-2^{n/2}$, pues, por ejemplo, para n=8 se sabía de funciones booleanas balanceadas con no linealidad de $112=2^{8-1}-2^{8/2}$. Sin embargo, en [16] se reportó una función booleana de 10 variables de entrada con no linealidad de $492=2^{10-1}-2^{10/2}+12$, valor que ya había sido predicho en [30] como el máximo teóricamente posible para funciones balanceadas de ese número de variables.

Por otro lado, en 1972 y en 1980 se demostró que la máxima no linealidad alcanzable con funciones booleanas de 5 y 7 variables es de 12 y 56, respectivamente, por lo que se supo que para $n\leq 7$ impar la máxima no linealidad para funciones de n variables es $2^{n-1}-2^{(n-1)/2}$ y se planteó la conjetura de si acaso ese valor se mantendría para n impar $n\geq 9$ [16].

Sin embargo, en 1983, tal conjetura fue refutada al hallarse que existen funciones

Tabla V. Cotas superiores teóricas y mejores valores alcanzados para no linealidad en funciones booleanas balanceadas

	5	6	7	8	9	10	11	12
Cota superior teórica	12	26	56	118	244	492	1000	2014
Mejor caso reportado	12	26	56	116	241	492	992	2010

> Las perspectivas en torno al problema combinatorio son muy prometedoras, pues desde hace unos tres años experimentamos una etapa de desarrollo acelerado, en la que en periodos muy cortos se anuncian nuevos y espectaculares resultados. No es aventurado predecir que en los próximos años se encontrarán muchas funciones booleanas con características criptográficas aún mejores que las reportadas hasta ahora, gracias al empleo de algoritmos y heurísticas evolutivas cada vez más sofisticados.

booleanas de 15 variables con no linealidad de $16276 = 2^{15-1} - 2^{(15-1)/2} + 20$. Este descubrimiento fue utilizado para demostrar que para n impar con $n \geq 15$, las funciones booleanas alcanzan una no linealidad de al menos $2^{n-1} - 2^{(n-1)/2} + 20 \cdot 2^{(n-15)/2}$.

Con estos resultados, el valor exacto de la máxima no linealidad alcanzable para n=9,11,13, quedó como un problema abierto, puesto que los mejores resultados que se conocían apuntaban a funciones booleanas con no linealidad de $2^{n-1} - 2^{(n-1)/2}$. Sin embargo, como se mencionó al final de la sección anterior, el año pasado, utilizando una búsqueda exhaustiva en subespacios restringidos FBRS, se reportó en [17] que para n=9 existen funciones con no linealidad $241 = 2^{9-1} - 2^{(9-1)/2} + 1 \cdot 2^{(9-9)/2}$.

Por ser 241 un número impar, este hallazgo permite conjeturar que acaso el valor máximo de no linealidad para funciones booleanas con 9 variables deba ser mayor o igual que 242.[22]

A manera de resumen general, en la tabla V se enlistan las cotas superiores teóricas y mejores valores reportados para la no linealidad de funciones booleanas balanceadas.

Con respecto a resultados de funciones booleanas con otras propiedades criptográficas (además de balance y no linealidad), únicamente mencionamos dos resultados interesantes, ambos reportados el año pasado. Utilizando el método de inversión espectral junto con la heurística evolutiva de cúmulo de partículas [18-19] se encontró una familia de funciones booleanas de 9 variables con perfil (9,3,5,240), esto es, con orden de inmunidad 3, orden algebraico 5 y no linealidad 240 [28]. Con este hallazgo se contestó afirmativamente una conjetura sobre la existencia de tales funciones lanzada desde el año 2000 en [30]. Un segundo resultado significativo se reportó en [1], donde se determinó que existen exactamente 36 y 10272 funciones del tipo FBRS con perfiles criptográficos de (7,2,4,56) y (8,1,6,116), respectivamente.[23]

A manera de conclusión señalamos que en los últimos tres años se han encontrado funciones booleanas con excelentes propiedades criptográficas, las cuales han permitido confirmar/refutar diversas conjeturas planteadas desde hacía más de tres décadas. No es exagerado afirmar que este gran avance ha sido posible gracias al círculo virtuoso conformado por la combinación de ingeniosos y refinados resultados combinatorios teóricos junto con el empleo de poderosos motores de búsqueda heurísticos (esencialmente a través de técnicas evolutivas).

Consideramos que las perspectivas con respecto a este ilustre problema combinatorio son muy prometedoras, pues desde hace unos tres años hemos entrado de lleno en una etapa de desarrollo acelerada, en la que en periodos muy cortos se anuncian nuevos y espectaculares resultados. No es aventurado predecir que en los próximos años se encontrarán muchas funciones booleanas con características criptográficas aún mejores que las reportadas hasta ahora, gracias al empleo de algoritmos y heurísticas evolutivas cada vez más sofisticados.

Por último, nos gustaría finalizar este manuscrito con una pregunta que consideramos obligada:

¿Se harán algunos de los descubrimientos de nuevas y mejores funciones booleanas en México y, más específicamente, en el **Cinvestav**?

Nos atrevemos a conjeturar que sí.

Agradecimientos

El autor de este artículo desea hacer público su agradecimiento a los doctores Nareli Cruz Cortés y Guillermo Morales-Luna por sus valiosos comentarios y sugerencias que ayudaron a mejorar el contenido y la forma de este artículo. ●

[Notas]

1 En la sección 2 se describen de manera general los cifradores por bloque; y en la sección 3 se define la propiedad de *no linealidad* (en el contexto de cifradores por bloque) de manera formal.
2 En la Sección 3 se presentan las definiciones formales de estas propiedades.
3 El estudio de los modos de operación en cifradores por bloque está fuera del enfoque de este artículo. Para una descripción más amplia de los modos de operación en cifradores por bloques se recomienda el excelente artículo introductorio en:
http://en.wikipedia.org/wiki/Block_cipher_modes_of_operation.
4 National Institute of Standards and Technology, http://www.nist.gov/.
5 El número de llaves secretas crece cuadráticamente con el número n de usuarios en el sistema, dado que necesita un intercambio de $n(n-1)/2$ llaves para que todas las entidades puedan comunicarse unas con otras de manera confidencial.
6 De acuerdo con la información pública que se tiene sobre el diseño de DES, se decidió que las cajas *S* tuvieran 6 bits de entrada y 4 de salida, por ser el máximo valor práctico que permitía la tecnología de la época (mediados de los años 70) [27].
7 Esta propiedad, conocida como *criterio de avalancha*, se discute formalmente en la siguiente sección.
8 Se especula que la estadounidense agencia nacional de seguridad (NSA por sus siglas en inglés) quiso, de manera sigilosa, reservarse la capacidad de *romper* DES cuando así lo estimara necesario, una inquietante posibilidad que fue sospechada desde siempre por grupos activistas [32-33].
9 Puesto que existen métodos eficientes que combinan *m* funciones booleanas de *n* bits para que juntas conformen una caja *S* de m-bits de salida.
10 La operación Or-Exclusiva (XOR, $\oplus$) consiste en la adición módulo 2 de dos variables de un bit cada una.
11 Dado que: $F(\omega)\big|_{\omega=0} = \sum_{x\in Z_2^n}(-1)^{f(x)\oplus x\omega} = \sum_{x\in Z_2^n}(-1)^{f(x)\oplus 0} = \sum_{x\in Z_2^n}(-1)^{f(x)}$, y es fácil ver que si efectivamente *f* es una función balanceada, la anterior sumatoria se hace cero.
12 Véase el ejemplo 2 y la figura 4 en la siguiente subsección.
13 Funciones *Bent* en inglés.
14 puesto que $F(0) \neq 0$.
15 Un valor de no linealidad 2 corresponde a la máxima no linealidad alcanzable por una función booleana de tres entradas.
16 *Strict avalanche criterion* (SAC).
17 A propósito de los conflictos entre las propiedades, desde hace mucho tiempo se sabe que para funciones booleanas balanceadas se cumple siempre que m+d≤n-1 [3].
18 Note que el método de inversión espectral supone que en un principio no se conoce el valor de tal función booleana.
19 En caso que $\hat{p}(x) = 0$ el valor correspondiente de $\hat{b}(x)$ se escoge aleatoriamente.
20 Máximo valor de no linealidad para funciones de siete entradas.
21 En inglés: *Rotation Symmetric Boolean Functions*.
22 Esta conjetura estaría sustentada en el hecho de que los valores de las máximas no linealidades teóricas conocidas hasta ahora son todos números pares, por lo que se piensa que un valor impar, como el obtenido en [17], es de alguna manera antiestético y hasta *contra natura* [29].
23 Todas esas funciones toman un valor $f(0)=0$ en el dominio booleano.

[Referencias]

[1] Carlet, C., D.K. Dalai, K.C. Gupta y S. Maitra. Algebraic Immunity for Cryptographically Significant Boolean Functions: Analysis and Construction. *IEEE Transactions on Information Theory* 52(7): 3105-3121, 2006.
[2] Chen, H. y D.G. Feng. An effective genetic algorithm for finding highly nonlinear boolean functions. En *CEC 2004: International Conference on Evolutionary Computation, Portland OR, USA, June 2004*, pp. 2120-2123. IEEE, 2004.
[3] Clark, J.A., J.L. Jacob, S. Maitra y P. Stnic. Almost boolean functions: The design of boolean functions by spectral inversion. *Computational Intelligence* 20 (3):450-462, 2004.
[4] Clark, J.A., J.L. Jacob y S. Stepney. The design of S-boxes by simulated annealing. En *CEC 2004: International Conference on Evolutionary Computation, Portland OR, USA, June 2004*, pp. 1533-1537. IEEE, 2004.
[5] Clark, J.A., J. L. Jacob, S. Stepney, S. Maitra y W. Millan. Evolving Boolean functions satisfying multiple criteria. *Proceedings of the Third International Conference on Cryptology*, pp. 246-259. Springer-Verlag, 2002.
[6] Cruz-Cortés, N. Comunicación personal inédita, diciembre 2006.
[7] Daemen, J. y V. Rijmen. *The Design of Rijndael*. Springer-Verlag New York, Inc., 2002. ISBN:3540425802.
[8] Díaz-Pérez, A., N.A. Saqib y F. Rodríguez-Henríquez. Some Guidelines for Implementing Symmetric-Key Cryptosystems on Reconfigurable-Hardware. En *IV Jornadas de Computación Reconfigurable y Aplicaciones*, pp. 379-387, septiembre 2004.
[9] Forré, R. Methods and instruments for designing s-boxes. *J. of Cryptology*, 2(3):115-130, 1990.
[10] Fuller, J., W. Millan y E. Dawson. Multiobjective optimization of bijective s-boxes. En *CEC 2004: International Conference on Evolutionary Computation, Portland OR, USA, June 2004*, pp. 1525-1532. IEEE, 2004.
[11] Gupta, K.C. y P. Sarkar. Improved construction of nonlinear resilient s-boxes. En *Proceedings of the 8th International Conference on the Theory and Application of Cryptology and Information Security*, pp. 466--483. Springer-Verlag, 2002.
[12] Hernández-Castro, J.C., P. Isasi y C. Luque del Arco-Calderón. Finding efficient nonlinear functions by means of genetic programming. En *KES 2003*, Seventh International Conference on Knowledge-Based Intelligent Information & Engineering Systems, pp. 1192-1198, 2003.
[13] Hernández-Luna, E. Documento de propuesta doctoral, enero 2005.
[14] Hernández-Luna, E. Criterio de avalancha estricto en funciones booleanas. Reporte técnico, mayo 2005.
[15] Hernández-Luna, E., C.A. Coello Coello y A. Hernández-Aguirre. On the use of a population-based particle swarm optimizer to design combinational logic circuits. En Ricardo S. Zebulum, David Gwaltney, Gregory Hornby, Didier Keymeulen, Jason Lohn y Adrian Stoica (eds.), *Proceedings of the 2004 NASA/DoD Conference on Evolvable Hardware*, pp. 183-190. IEEE Computer Society, junio 2004.
[16] Kavut, S., S. Maitra, S. Sarkar y M.D. Yücel. Enumeration of 9-Variable Rotation Symmetric Boolean Functions Having Nonlinearity > 240. Rana Barua, Tanja Lange (eds.), Progress in Cryptology - INDOCRYPT 2006, 7th International Conference on Cryptology in India, Proceedings. Lecture Notes in Computer Science, vol. 4329, pp. 266-279, Springer, 2006.
[17] Kavut, S., S. Maitra y S. Sarkar. There exist Boolean functions on n (odd) variables having nonlinearity > $2^{n-1} - 2^{n-1/2}$ if and only if n > 7, Cryptology ePrint Archive, Report 2006/181. Disponible en: http://eprint.iacr.org/, 2006.
[18] Kennedy, J. y R.C. Eberhart. Particle Swarm Optimization. En *Proceedings of the 1995 IEEE International Conference on Neural Networks*, pp. 1942-1948, Piscataway, New Jersey, 1995. IEEE Service Center.
[19] Kennedy, J. y R.C. Eberhart. *Swarm Intelligence*. Morgan Kaufmann Publishers, San Francisco, California, 2001.
[20] López-Trejo, E., F. Rodríguez-Henríquez y A. Díaz- Pérez. An Efficient FPGA implementation of CCM Using AES. The 8th International Conference on Information Security and Cryptology (ICISC'05), Lecture Notes in Computer Science, vol. 3935, pp. 208-215, 2005.
[21] Menezes, A.J., S.A. Vanstone y P.C. Van Oorschot. *Handbook of Applied Cryptography*. CRC Press, Inc., 1997. ISBN: 0-8493-8523-7.
[22] Millan, W., J. Fuller y E. Dawson. Evolutionary generation of bent functions for cryptography. En Ruhul Sarker, Robert Reynolds, Hussein Abbass, Kay Chen Tan, Bob McKay, Daryl Essam y Tom Gedeon (eds.), *CEC*, pp. 149-158, Canberra, 8-12, IEEE Computer Society Press, diciembre 2003.
[23] Millan, W., J. Fuller y E. Dawson. New concepts in evolutionary search for boolean functions in cryptology. In *Computational Intelligence* 20(3): 463-474, 2004.
[24] NIST. Announcing the Advanced Encryption Standard (AES). Federal Information Standards Publication, noviembre 2001. Disponible en: http://csrc.nist.gov/CryptoToolkit/aes/index.html
[25] Pieprzyk J. y C.X. Qu. Fast hashing and rotation-symmetric functions. *Journal of Universal Computer Science* 5(1):20-31, 1999.
[26] Rodríguez-Henríquez, F., N.A. Saqib y A. Díaz-Pérez. 4.2 Gbit/s Single-Chip FPGA Implementation of AES Algorithm. *Electronic Letters* 39(15): 1115-1116, julio 2003.
[27] Rodríguez-Henríquez, F., N.A. Saqib, A. Díaz Pérez y Ç.K. Koç. *Cryptographic Algorithms on Reconfigurable Hardware*, Springer First Edition, noviembre 2006. ISBN: 0387338837.
[28] Saber, Z., M.F. Uddin y A. Youssef. On the existence of (9, 3, 5, 240) resilient functions. *IEEE Transactions on Information Theory* 52(5): 2269-2270 (2006).
[29] Sarkar, P. Comunicación personal (a través de D. Chakraborty) inédita, diciembre 2006.
[30] Sarkar P. y S. Maitra. Nonlinearity bounds and construction of resilient Boolean functions. En *Advances in Cryptology - Crypto 2000*, pp. 515-532, Berlin, 2000. Springer-Verlag. Lecture Notes in Computer Science, vol. 1880.
[31] Schneier, B. *Applied Cryptography. Protocols, Algorithms, and Source Code in C*. John Wiley & Sons, segunda edición, 1996. ISBN 0-471-11709-9.
[32] Singh, S. The Code Book. Fourth Estate. Segunda edición, junio 2000. ISBN 978-1857028898. Disponible en:http://www.simonsingh.net/[33] Singh, S. Los códigos secretos. Debate, 2000. ISBN: 84-8306-278-X.
[34] StDnicD, P., S. Maitra y J. Clark. Results on Rotation Symmetric Bent and Correlation Immune Boolean Functions. Fast Software Encryption Workshop (FSE 2004), Nueva Delhi, INDIA, LNCS 3017, Springer Verlag, pp. 161-177, 2004.
[35] StDnicD, P. y S. Maitra. Rotation symmetric Boolean functions – Count and cryptographic properties. En R.C. Bose Centenary Symposium on Discrete Mathematics and Applications, December 2002, Indian Statistical Institute, Calcutta and Technical Report of Cryptology Research Group, Reporte técnico CRG/2002/10, noviembre 2002. Disponible en: http://www.isical.ac.in/~crg/tech_reports.html.

Distinciones Académicas 2006

El **Cinvestav** extiende sus más cálidas felicitaciones a sus investigadores, estudiantes y auxiliares de investigación, por las distinciones académicas alcanzadas en 2006, año en el que se graduaron 298 estudiantes de Maestría y 168 de Doctorado, en sus programas de Posgrado, los cuales se encuentran registrados en el Padrón Nacional de Posgrados de SEP-Conacyt.

Dr. Adolfo Martínez Palomo
Miembro del Comité Internacional de Bioética de la UNESCO, con sede en París

Dr. Eduardo José Bayro Corrochano
Dr. Fernando José Esparza García
Dra. Ana Carmela Ramos Valdivia
Dra. María de la Luz del Razo Jiménez
Dr. José Oscar Rosas Ortiz
Dr. José Víctor Segovia Vila
Dr. Eduardo Johann Weiss Hoz
Ingreso como Miembros de la Academia Mexicana de Ciencias

Dr. Adolfo Martínez Palomo, Dra. María de Ibarrola Nicolín y Dr. Pablo Rudomín
Miembros del Consejo de Especialistas para la Educación (Codese), para asesorar al Secretario de Educación Pública en materia de planeación y política educativa

Dra. Antonia Candela Martín
Representante del Cinvestav en el Consejo Consultivo Interinstitucional para el Desarrollo de la Asignatura de Ciencias de la SEP

Dra. Esther Orozco Orozco
Designada como Directora del Instituto de Ciencia y Tecnología del Gobierno del Distrito Federal

Dr. José Luis Leyva Montiel
Premio Estatal de Ciencia y Tecnología, por el trabajo: *Alliance, Sistema Telefónico VoIP para Telefonía Rural*, correspondiente al área de Desarrollo Industrial y Manufactura

Dr. Pavel Zúñiga Haro
Premio Estatal de Ciencia y Tecnología de Jalisco 2006, en la categoría de Ciencia, por el trabajo: *Análisis y control de un compensador serie*, correspondiente al área de Desarrollo Industrial y Manufactura

Dr. Yasuhiro Matsumoto Kawabara
Ing. José Antonio Urbano Castelán (Auxiliar de Investigación) Segundo lugar en la categoría de la innovación en el III Premio Nacional de Energía Renovable, que otorga la Secretaría de Energía y la Comisión Nacional para el ahorro de Energía por su trabajo: *Estufa Rural de Concentración Solar*

Dr. Pablo R. Hernández Rodríguez
Título de Patente No. 238476, por la invención del *Sistema digital de ayuda para la comunicación de personas con discapacidad en el lenguaje utilizando voz sintética*

Dr. José Mustre de León
Vicepresidente de la Sociedad Mexicana de Física a partir de 2007, en el XLIX Congreso Nacional de Física

Dr. Gregorio Toscano Pulido (Estudiante)
Dr. Carlos A. Coello Coello (Tutor)
Primer Lugar de la categoría única de nivel doctorado del XIX Certamen Nacional de Tesis de la Asociación Nacional de Instituciones de Educación en Informática (ANIEI) 2006, por el trabajo: *Uso de auto adaptación y elitismo para optimización multiobjetivo mediante cúmulos de partículas*

Dr. Gerardo Herrera Corral
Premio a la Investigación Científica 2006 otorgado en el XLIX Congreso Nacional de Física, por la Sociedad Mexicana de Física en *Reconocimiento a su trayectoria científica*

M. en C. Elsa Monroy Ordoñez (Estudiante)
Dr. David Centurión (Tutor)
Premio Nacional Jaime Herrera 2006 de la Sociedad de Hipertensión Arterial de México A.C., en el área de Investigación Básica, por el trabajo de tesis: *Caracterización farmacológica de los mecanismos involucrados en la inhibición de algunas imidazolinas sobre las respuestas vasopresoras inducidas por la estimulación simpática en la rata descerebrada y desmedulada*

M. en C. Eugenio Vidal Granel (Estudiante)
Dr. Fernando Navarro García (Tutor)
The ASM Student and Post Doctoral Travel Grant de la American Society of Microbiology y el ICAAC Program Committee, así como el premio Corporate Activities Program Student Travel Grant por el trabajo: *Type III Secretion System (TTSS) Helps to Translocate EspC Autotransporter Protein from Enteropathogenic Escherichia coli (EPEC) to the Eukaryotic Cell*

Dra. Guadalupe Ortega Pierres (Investigadora)
Dra. Marisela Cruz Soto,, Dr. Raúl Arguello García y Arturo Pérez Taylor (Auxiliares de Investigación)
Mención especial en el área de investigación básica del Premio Canifarma 2005 por el trabajo: *Caracterización in vitro de mecanismos moleculares de resistencia a Albendazol en trofozoitos Giardia duonenalis*

Dra. Esther Orozco Orozco
"Medalla al Mérito Científico en Ciencias y Artes", otorgado por la Comisión de Ciencia y Tecnología, de la Asamblea Legislativa del D.F.

Dra. Rosa Ma. Farfán Márquez
Reconocimiento que le hace la Universidad de Camaguey, en Cuba, por su dedicación y entrega al desarrollo del movimiento latinoamericano de la Matemática Educativa

M. en C. Nancy Margarita Costas Cáceres (Estudiante)
The Presidencial Award for Excellence in Mathematics and Sciences Teaching, premio más alto que se otorga a un maestro en los Estados Unidos

Bióloga Ruth Reyes Cortés (Estudiante)
Dra. Mireya de la Garza Amaya (Tutora)
Student Travel Grant por el trabajo: *Bacteriophages specific to Pasteurella multocida D*, en la American Society for Microbiology Conference on Pasteurellacease 2005

M. en C. Ana Belem Piña Guzmán (Estudiante)
Dra. Betzabet Quintanilla Vega (Tutora)
Hispanic Organization for Toxicologists Scientific Achievement Award por el trabajo: *Methylparathion induces sperm DNA damage in mice*, presentado en el 45° Congreso Anual de la Sociedad de Toxicología de los Estados Unidos

Centro de Investigación y de Estudios Avanzados del Instituto Politécnico Nacional

Cinvestav

Dr. José Antonio Ruz Hernández (Estudiante)
Dr. Edgar Sánchez Campero (Tutor)
Primer lugar de tesis de doctorado en Informática y Control del XVIII Certámenes Nacionales de Tesis 2005-2006 que otorgan el Instituto de Investigaciones Eléctricas de la Comisión Federal de Electricidad y el Fideicomiso para el Ahorro de Energía, con el trabajo: *Esquema neuronal para detección y diagnóstico de fallas en centrales termoeléctricas*

Dra. Nidia Maribel León Sicairos (Estudiante)
Dra. Mireya de la Garza Amaya (Tutora)
Rainee Award por su trabajo: *Microbicidal mechanism of lactoferrin and lactoferricin B and their synergistic effect with metronidazole in Entamoeba histolytica*, en el 7th International Conference on Lactoferrin: Structure, Function and Applications
& ASM Student and Post Doctoral Travel Grant de la American Society for Microbiology (ASM) y el ISAAC Program Committee, por el trabajo: *Characterization of the microbicidal activity of lactoferrin in Entamoeba histolytica*

M. en C. Olga Lidia Valenzuela Limón (Estudiante)
Dra. Ma. de la Luz del Razo Jiménez (Tutora)
Student Award for Outstanding Presentation in Risk assessment, Specialty Section
& Graduate Student Travel Award por el trabajo: *Relation of urinary metabolites of inorganic arsenic with transforming growth factor alpha concentration in bladder urothelial cells from a population environmentally exposed to inorganic arsenic*, presentado en el 45o. Congreso Anual de la Sociedad de Toxicología de los Estados Unidos

Dr. Rafael Villalobos Molina
Premio Martín de la Cruz de investigación química y biología aplicada al conocimiento en el desarrollo de fármacos que otorga el Consejo de Salubridad General, en reconocimiento a su trabajo en favor de la salud de la población mexicana

Dr. Eduardo José Bayro Corrochano
Distinguido con el Fellow for contributions to geometric computing for perception action systems, otorgado por la International Association for Pattern Recognition

Dr. Vinicio Granados Soto
Keith F. Killam Jr. Memorial Award, otorgado por la Western Pharmacology Society a jóvenes investigadores

M. en C. Norma Elena Pérez Herrera (Estudiante)
Dra. Ma. Betzabet Quintanilla Vega (Tutora)
Primer lugar de presentación oral dentro de la X Reunión Nacional de Investigación en Salud en el Trabajo, con la exposición: *Efectos de la salud reproductiva de trabajadores agrícolas ocupacionalmente expuestos a plaguicidas*
& Mención honorífica por la conferencia: *Continuos occupational exposure to pesticidas alters semen quality and sperm DNA integrity*, presentado en la 18th. Conference of the International Society for Environmental Epidemiology

M. en C. Raúl Martínez Memije (Estudiante)
Dr. Ernesto Suaste Gómez (Tutor)
Reconocimiento especial en el área de soluciones clínicas innovadoras por el trabajo: *Heart rate variability and pupilar area variability analisis in health an diabetics*, presentado en el Panamerican Health Care Engineering Conference 2006

Dr. Pedro Joseph-Nathan
Nombramiento como Profesor Honorario de la Facultad de Ingeniería de la Universidad Nacional de Jujuy, San Salvador de Jujuy, República de Argentina: por su aporte a la generación del conocimiento en el campo de la Química de los Productos Naturales

Dra. Rossana Arroyo Verástegui y colaboradores
Primer lugar del XVII Premio Nacional de Investigación de la Fundación Glaxo Smith Kline, en el área de Investigación Básica con el trabajo: *Mecanismo alternativo de regulación de la expresión génica por hierro en Tricomonas vaginalis*

M. en C. José Merced Lozano García (Estudiante)
Dr. Edgar Sánchez Campero (Tutor)
Primer lugar de tesis de maestría en Redes Eléctricas en el XVIII Certamen Nacional de Tesis 2005-2006 que otorgan el Instituto de Investigaciones Eléctricas, la Comisión Federal de Electricidad y el Fideicomiso para el Ahorro de Energía, con el trabajo: *Compensador estático serie para el mejoramiento de la calidad de energía de redes eléctricas*

Dr. Pável Zuñiga Haro (Estudiante)
Dr. Juan Manuel Ramírez Arredondo (Tutor)
Primer lugar de tesis de doctorado en Redes Eléctricas del XVIII Certámenes Nacionales de Tesis 2005-2006 que otorgan el Instituto de Investigaciones Eléctrica, la Comisión Federal de Electricidad y el Fideicomiso para el Ahorro de Energía, con el trabajo: *Análisis y control de un compensador serie*

Dra. Esther López Bayghen
Primer lugar del XVII Premio Nacional de Investigación de la Fundación Glaxo Smith Kline, en el área de investigación clínica, por el trabajo: *Reconstrucción de vaginas humanas; primer reporte clínico de fabricación exitosa de vagina humana con tecnología de ingeniería de tejidos*

Dra. Luz Abril Torres Méndez
Primer Lugar en el Best paper award por el trabajo: *Statics of visual and partial depth data for mobile robot environment modeling*, presentado en el Fifth Mexican International Conference on Artificial Intelligence (MICAI'06), Apizaco, Tlax.

Dr. Jaime Ortega López
Título Honorífico de Profesor Visitante, diploma de reconocimiento y medalla, otorgado por el Consejo Universitario de la Universidad Nacional de San Cristóbal de Huamanga, Perú

Dr. Luis Gabriel Brieba de Castro
Dr. Luis Herrera Estrella
Dr. Jean Phillipe Vielle Calzada
Seleccionados como International Research Scholar por la Howard Hughes Medical Institute

I.Q.I. Melchor Martínez Herrera (Estudiante)
Dr. Aarón Rojas Aguilar (Tutor)
IUPAC Poster Prize por el trabajo: *Molar standard enthalpies of combustion and formation of the fullereen C84*, presentado en la 19th International Conference on Chemical Thermodynamics que organiza la International Union on Pure and Applied Chemistry, en Colorado, EUA

Reconocimiento del Club de Rotarios Vallejo por la actividad de servicio en bien de la Comunidad:
Dra. Silvia Lorenia Cruz Martín del Campo,
por su trabajo en el área de las adicciones y trabajo con el Centro Nacional de Adicciones
Dr. Heriberto Cuanalo de la Cerda,
por el trabajo centrado en el combate a la pobreza aplicado en comunidades pobres del Estado de Yucatán
Dra. Angelina Flores Parra,
por su contribucción en forma sobresaliente en la difusión de la ciencia y la educación en niños a nivel primaria y secundaria
Dr. Romeo de Coss Gómez,
por el impulso a las Olimpiadas de Física y la preparación de estudiantes de preparatoria

Dra. Libia Vega Loyo
Reconocimiento como revisora para el *American Journal of Epidemiology*, del Dr. Moisés Szklo, Editor en Jefe

Dr. Pablo Muriel de la Torre
Incorporación al Comité Editorial del *Journal of Applied Toxicology*

Dr. Eusebio Juaristi Cosio
Incorporación al Consejo Editorial del *Journal of Physical Organic Chemistry*

Dra. Rosa María Bermúdez Cruz
Dr. Gabriel Guarneros Peña
Dr. Luis Y. Kameyama Kawabe
M. en C. Eva Martínez Peñafiel (Estudiante)
Premio al mejor trabajo libre en el XXV Congreso Nacional de Microbiología por el cartel: *Investigación de la relación entre la expresión de la hemolisina silenciosa SheA de Escherichia coli y uno de los productos (ORF4) del bacteriófago mEp021*

Dr. Romeo de Coss Gomez y colaboradores
Medalla de Oro en la XVII Olimpiada Nacional de Física, que se llevó a cabo en Durango.
Primer lugar en equipos en la participación por el Estado de Yucatán

M. en C. Alejandro Altamirano Gutiérrez
M. en C. Edgar Jesús Borja Arco
M. en C. Jorge Uribe Godínez (Estudiantes)
Primer lugar del mejor stand en la Expo-energía del XVII Congreso Nacional de Ahorro de Energía otorgado por el Colegio de Ingenieros Mecánicos y Electricistas del Estado de Jalisco, A.C.

Dr. Jorge Hernández Rodríguez
Premio de Investigación sobre Defectos al Nacimiento en la categoría de Investigación Biomédica básica por el trabajo: *Prenatal Impairment of Brain Serotonergic transmission in Infants*, otorgado por el Grupo de Estudios del Nacimiento, A. C.

www.cinvestav.mx

En la construcción de la Univac I se utilizó un invento revolucionario de John Presper Eckert, mismo que condenó a la obsolescencia a las tarjetas perforadas de IBM, pues la entrada y salida de datos se efectuaba por medio de cintas magnéticas. El precio comercial de la *Universal Automatic Computer* era de 750 mil dólares.

Figura 1. En esta imagen se muestra a la Univac I junto con su operador. De pie puede verse, de izquierda a derecha, a John Presper Eckert (diseñador principal de la Univac I) y a Walter Cronkite (presentador de noticias de la CBS) durante la noche de la elección presidencial de 1952.

El origen del miedo a las computadoras

EN OCASIÓN DE LAS ELECCIONES PRESIDENCIALES DE 1952, LA AUDIENCIA TELEVISIVA DE ESTADOS UNIDOS TUVO LA OPORTUNIDAD DE VER POR PRIMERA VEZ EL ASPECTO DE UNA COMPUTADORA ELECTRÓNICA. LA LLAMADA UNIVAC I MEDÍA 3 METROS DE LARGO, 4.20 DE ANCHO Y 2.70 DE ALTO Y PESABA 8 TONELADAS; ESTABA DESTINADA A PREDECIR EL RESULTADO DE LA CONTIENDA ELECTORAL.

Carlos A. Coello Coello

La Univac I[1] fue todo un hito en la historia de la computación, no sólo por haber sido la primera computadora electrónica de propósito general que se comercializó en los Estados Unidos (la primera se vendió en 1951), sino también por sus innovaciones tecnológicas [3]. La computadora fue concebida como el proyecto principal de la empresa *Eckert-Mauchly Computing Corporation* (EMCC). Sin embargo, tras enfrentar una grave crisis financiera, en 1950 la EMCC fue adquirida por la Remington Rand, empresa que se responsabilizaría de su comercialización.

La memoria de la Univac I se implementó usando líneas de retardo de mercurio y tenía capacidad para almacenar hasta mil palabras de 12 caracteres cada una. Su arquitectura era serial y bastante conservadora pero, dado que su ciclo de reloj era de 2.25 megahertz, su alta velocidad compensaba por cualquier restricción que pudiera imponer su diseño. La Univac I usaba, además, sólo 5 mil bulbos, que contrastaban con los 18 mil de la legendaria ENIAC[2] [4]. Sus dimensiones eran 3.00 x 4.20 x 2.70 metros, lo que la hacía relativamente pequeña comparada con sus competidores de aquellos días (aunque su peso era de unas 8 toneladas). La entrada y la salida de datos se efectuaba por medio de cintas magnéticas, usando un invento revolucionario de John Presper Eckert que condenó a la obsolescencia a las tarjetas perforadas de IBM, tan populares en esa época. La cinta tenía 1.27 centímetros de ancho y entre 0.00254 y 0.00762 centímetros de espesor y cada carrete alojaba 360 metros de cinta, permitiendo almacenar en un área relativamente reducida más de un millón de caracteres. Su precio comercial era de aproximadamente 750 mil dólares, sin incluir los dispositivos de entrada y salida (por ejemplo, una impresora de alta velocidad costaba 185 mil dólares).

Pero, a pesar de todos sus adelantos tecnológicos, la Univac I se vendió poco en un principio y fue debido a un fortuito evento y no a sus innovaciones que la palabra Univac llegó a convertirse en sinónimo de computadora durante muchos años, en un reflejo de su enorme popularidad.[3]

Este evento, ahora muy famoso, fue no sólo la primera aparición de una computadora frente a las cámaras de televisión, sino que marcó también el inicio del temor de los humanos hacia las computadoras, el cual luego sería agudizado en la literatura y el cine de

CARLOS ARTEMIO COELLO COELLO En 1996 se doctoró en Ciencias de la Computación en la Universidad Tulane (Estados Unidos). Es Investigador 3-D y Jefe del Departamento de Computación del **Cinvestav**. Pertenece al Sistema Nacional de Investigadores, nivel 3, y es miembro de la Academia Mexicana de Ciencias. Ha publicado más de 180 artículos en revistas y para congresos internacionales con arbitraje estricto. Es coautor del libro *Evolutionary Algorithms for Solving Multi-Objective Problems* (Kluwer Academic Publishers, 2002) y coeditor del libro *Applications of Multi-Objective Evolutionary Algorithms* (World Scientific, 2004), y autor del libro de divulgación *Breve historia de la computación y sus pioneros* (FCE, 2003). Sus publicaciones reportan más de 850 citas en el *ISI Citation Index*. Es editor asociado de las revistas *IEEE Transactions on Evolutionary Computation* (IEEE Press), *Evolutionary Computation* (MIT Press), *Journal of Heuristics* (Springer) y *Computational Optimization and Applications* (Springer).
ccoello@cs.cinvestav.mx

ciencia ficción. Me refiero, por supuesto, a la elección presidencial de 1952 en los Estados Unidos.

En 1952, la empresa Columbia Broadcasting System (CBS) le pidió a la Remington Rand algunas sumadoras e impresoras para efectuar sus estimaciones sobre quién ganaría las elecciones presidenciales. A cambio, la CBS le prometió a la Remington mostrar el logotipo de la empresa ante las cámaras, para hacerle publicidad [2].

Alguien del departamento de relaciones públicas de la Remington sugirió mejor el uso de una Univac I para efectuar el conteo, pensando que así podrían publicitar su máquina. Se le ofreció entonces a la CBS que se montara un pequeño espectáculo que demostrara el poder de cálculo de la máquina. La CBS accedió, pero tomó con cautela la sugerencia de que la computadora predijera al ganador de la elección, dado lo delicado del asunto y la desconfianza que los ejecutivos de la cadena televisiva tenían en la máquina.

En una tarea aparentemente sin precedente en la historia de los Estados Unidos, los ingenieros de la Remington alimentaron con miles de datos estadísticos de elecciones pasadas (desde 1928) a la Univac I, usando además la asesoría de politólogos que les indicaban qué datos eran relevantes y cuáles no [2].

Temerosos de hacer el ridículo, los ingenieros de la Remington decidieron utilizar tres computadoras: una para procesar los datos cuando estuvieran al aire, otra para verificar sus resultados y una última para respaldo, en caso de que algo saliera mal con las otras dos. La información se transmitiría por medio de teletipos entre Nueva York y Filadelfia [1].

La CBS comenzó su transmisión a las seis de la tarde (tiempo de Nueva York) del 6 de noviembre de 1952, y los primeros resultados de la elección se enviaron por triplicado mediante teletipo y se transfirieron a tres cintas magnéticas. Si los resultados de las tres máquinas coincidían, entonces la información producida se almacenaba en una cuarta cinta. El programa que se escribió verificaba posibles inconsistencias de la información[4] y procesaba los datos de acuerdo con las tendencias históricas que la Univac I tenía almacenada. A las 8:30 de la noche y con sólo 7% de los votos totales procesados, la Univac I predijo una victoria arrolladora del candidato republicano Dwight D. Eisenhower sobre su contrincante demócrata Adlai E. Stevenson [1,2]. Eso desató un verdadero pandemónium en la Remington, porque lo que la Univac I predecía estaba contradiciendo lo que todos los expertos en política pensaban.[5] El reportero Charles Collingwood, que era el responsable del enlace televisivo con los operadores de la Univac I tuvo que salir del aire para poder decidir si daba esa información o no, mientras los ingenieros de la Remington verificaban por enésima vez su programa [2].

Arthur Draper, director de investigación de la Remington, ordenó a los ingenieros que modificaran el programa para que coincidiera con lo que los expertos en política predecían y, tras alterar un factor de extrapolación, los cálculos (todavía favorecedores a Eisenhower) resultaron un poco más conservadores. Tras una serie de ajustes posteriores al programa, se pudo hacer que la Univac I produjera finalmente una ventaja mínima de Eisenhower sobre Stevenson [2].

A las diez de la noche, la CBS transmitió los resultados alterados, respirando aliviados de que la computadora finalmente había coincidido con los expertos. Sólo una hora más tarde se hizo evidente que la Univac I había tenido razón, y la computadora, aun con todas las alteraciones sufridas en su programa, comenzó a dar una probabilidad de 100 sobre 1 de que Eisenhower ganaría. La CBS tuvo que salir nuevamente al aire y admitir públicamente lo que había ocurrido tras bambalinas, en un episodio por demás vergonzoso en el que el mismísimo presidente de la Remington Rand hubo de revelar las manipulaciones de que había sido objeto el programa de la Univac I [2].

Cuando todo el episodio concluyó, se supo que la Univac I había predicho, con sólo 7% de los votos procesados, que Eisenhower obtendría 438 distritos electorales y el conteo oficial arrojó la cifra 442, que estaba sólo 1% arriba de lo que la computadora estimó (Stevenson logró ganar únicamente en 89 distritos electorales). Cuentan que, desde entonces, la gente le tiene miedo a las computadoras.

[Notas]

[1] Univac es el acrónimo de *Universal Automatic Computer*.

[2] ENIAC son las siglas de *Electronic Numerical Integrator and Computer*, considerada como la primera computadora electrónica de uso general. Se diseñó y construyó en la Universidad de Pensilvania entre 1943 y 1945, aunque se presentó en público hasta febrero de 1946.

[3] Eventualmente se vendieron unas 46 unidades de la Univac I entre 1951 y 1957 [5]. La primera se vendió a la Oficina del Censo de los Estados Unidos. La computadora se entregó el 31 de marzo de 1951, pero fue hasta el 14 de junio en que comenzó a operar. Con motivo de tan singular evento se develó una placa conmemorativa.

[4] Por ejemplo, se verificaba que no hubiesen más votos que votantes registrados en un cierto distrito.

[5] Se suponía que los candidatos republicanos nunca ganaban en los estados del sur, y la computadora decía que ese no sería el caso de Eisenhower [1].

[Referencias]

[1] Shurkin, Joel. *Engines of the Mind. The Evolution of the Computer from Mainframes to Microprocessors*, W. W. Norton & Company, New York, 1996.

[2] Wulforst, Harry. *Breakthrough to the Computer Age*, Scribners, New York, 1982.

[3] Slater, Robert. *Portraits in Silicon*, The MIT Press, Cambridge, Massachusetts, 1992.

[4] Coello Coello, Carlos A. *Breve Historia de la Computación y sus Pioneros*, Fondo de Cultura Económica, México, 2003.

[5] Maynard, Michael M. "UNIVAC I", en Bryan Ralston and Edwin D. Reilly (eds.), *Encyclopedia of Computer Science*, pp. 1405-1406, Third Edition, Van Nostrand Reinhold, New York, 1993.

Nutrida con la información estadística de elecciones presidenciales del periodo anterior y con la asesoría de politólogos, la Univac I predijo, con sólo 7% de los votos procesados, una victoria arrolladora del candidato republicano Dwight D. Eisenhower sobre su contrincante demócrata Adlai E. Stevenson.

Foto de la Univac I, en donde se aprecia su enorme tamaño.

Vladimir Kharitonov en su oficina.

Vladimir Kharitonov, once años en México

EN 1995, EL DOCTOR KHARITONOV SE INCORPORÓ AL EQUIPO DE INVESTIGADORES DEL HOY DEPARTAMENTO DE CONTROL AUTOMÁTICO DEL **CINVESTAV**. DESPUÉS DE UNA CARRERA EXITOSA, REALIZADA EN LOS ÚLTIMOS ONCE AÑOS, EN LA CIUDAD DE MÉXICO, EL MATEMÁTICO REGRESA A SU NATAL RUSIA Y AL PUESTO QUE OCUPA EN LA UNIVERSIDAD DE SAN PETERSBURGO, DONDE, SEGURAMENTE, SEGUIRÁ SU DESEMPEÑO CIENTÍFICO CON EL MISMO ÉXITO.

Sabine Mondié Cuzange

Vladimir Kharitonov nació en Achinsk, Krasnoyrskii Krai (Rusia), en 1950. Se graduó en 1973 como Ingeniero en Matemáticas y empezó a trabajar en el Instituto de Matemáticas Numéricas y Teoría del Control de la Universidad Estatal de Leningrado. Obtuvo el grado de candidato al doctorado en ciencias en 1979, y se incorporó a la facultad como docente. Ahí presentó su tesis de doctorado en Ciencias, en 1990, y recibió un año después el título de Profesor de la Universidad.

El resultado científico más destacado de Kharitonov concierne al análisis de estabilidad robusta de polinomios [1]. El matemático mostró el hecho sorprendente de que se puede concluir que una familia intervalo de polinomios, que contiene un número infinito de éstos, es estable si únicamente cuatro elementos de esta familia, llamados polinomios de Kharitonov, son estables. Este teorema es útil en el campo de control robusto, donde se busca diseñar controladores que funcionan a pesar de las incertidumbres inherentes a los errores de modelado, medición y cambios en condiciones de operación. Por sus numerosas aplicaciones y extensiones, dicho teorema con más de 600 citas, le ha dado a su autor renombre internacional. En 1995, el Dr. Kharitonov se incorporó al equipo de investigadores del hoy Departamento de Control Automático del **Cinvestav** México, donde llegó a ser Investigador 3E y miembro del Sistema Nacional de Investigadores con nivel 3.

Las dotes pedagógicas sobresalientes de Vladimir se han hecho patentes en seminarios y cursos magistrales de una claridad notable, seguidos por alumnos y profesores sobre los temas de estabilidad, estabilidad robusta, teoría del control y sistemas con retardos, así como en el libro *Stability of Time-Delay Systems* [2], publicado en 2003, del cual es coautor. La puerta de la oficina de Vladimir siempre ha estado abierta para sus colegas y estudiantes. Aquél que cruzó su umbral, ya que según la superstición rusa es de mal agüero platicar con una puerta de por medio, jamás ha salido sin una respuesta...u otra pregunta.

Cabe mencionar el papel de liderazgo de Kharitonov en la actualización de los programas de maestría del departamento, así como su participación como

SABINE MONDIÉ CUZANGE Ingeniera Industrial y de Sistemas (ITESM), maestra en Ciencias (**Cinvestav**) y doctora en Ciencias, especialidad Control Automático (**Cinvestav** y Universidad de Nantes, Francia). Pertenece al Sistema Nacional de Investigadores, nivel 2. Sus líneas de investigación incluyen los sistemas con retardos, la estructura de sistemas lineales y el uso de la teoría de sistemas en problemas biológicos. Actualmente es investigadora titular del Departamento de Control Automático del **Cinvestav**, coordinadora académica del mismo y profesora regular de cursos de especialización en Control Automático y Teoría de Sistemas. Ha participado en publicaciones internacionales y libros, así como en presentaciones en congresos internacionales y nacionales. Es editora asociada de la revista *European Journal of Control*. Pertenece a diversas sociedades científicas, entre otras, Asociación de México de Control Automático y *System Control Society* de IEEE.
smondie@ctr.cinvestav.mx

Teorema de Kharitonov

Definición: Un polinomio intervalo es una familia de polinomios

$$p(s) = a_0 + a_1 s + a_2 s^2 + ... + a_n s^n$$

donde cada coeficiente $a_i \in R$ pertenece al intervalo $[l_i, u_i]$, $l_i \leq u_i$.
Se supone además que el coeficiente líder no puede ser cero: $0 \notin [l_n, u_n]$.

Teorema: Un polinomio intervalo es estable si y sólo si los cuatro polinomios de Kharitonov

$$\begin{aligned} k_1(s) &= l_0 + l_1 s + u_2 s^2 + u_3 s^3 + l_4 s^4 + l_5 s^5 + ... \\ k_2(s) &= u_0 + u_1 s + l_2 s^2 + l_3 s^3 + u_4 s^4 + u_5 s^5 + ... \\ k_3(s) &= l_0 + u_1 s + u_2 s^2 + l_3 s^3 + l_4 s^4 + u_5 s^5 + ... \\ k_4(s) &= u_0 + l_1 s + l_2 s^2 + u_3 s^3 + u_4 s^4 + l_5 s^5 + ... \end{aligned}$$

El teorema que trajo el reconocimiento internacional al Dr. Kharitonov.

presidente del comité de programa de diversos eventos científicos internacionales, en particular el II Symposium IFAC on System, Structure and Control, auspiciado por el Departamento de Control Automático en diciembre de 2004, en la ciudad de Oaxaca. Su trabajo de investigación en México se ha desarrollado en el marco de 9 tesis doctorales, dos de las cuales están por concluir, y 14 de maestría, dando lugar a más de 50 publicaciones en revistas de prestigio internacional.

Un primer eje de su trabajo de investigación en el **Cinvestav** se ubica en la continuación de su famosa contribución inicial con el estudio de familias de polinomios multivariables [3], útiles en el modelado de sistemas multidimensionales tales como métodos numéricos y procesamiento de imágenes. Las contribuciones en este campo van de la obtención misma de una definición satisfactoria de la estabilidad de los polinomios multivariables, compatible con propiedades de robustez como el teorema de las aristas, la estabilidad de familias intervalo (tesis de Marco Iván Ramírez Sosa Morán, ganadora del premio Arturo Rosenblueth en el año 2000), al estudio de correspondencias con la estabilidad en el sentido de Schur (tesis de Eduardo Rodríguez Ángeles), y también a la utilización de polinomios multivariables en el análisis de sistemas con retardos (tesis de Benjamín Ortiz Moctezuma).

Este tema está conectado de manera natural con el segundo eje de trabajo que Vladimir ha cultivado en estos años, los sistemas con retardos. Hoy en día, este tema es objeto de una intensa actividad científica, ya que los sistemas con retardos permiten modelar fenómenos de transporte de materia e información, tiempos de cálculo, y fenómenos de maduración en sistemas biológicos, entre otros.

Una de sus primeras aportaciones fue el descubrimiento de intrigantes dinámicas adicionales en el marco de la teoría de Lyapunov Krasovskii en la tesis de Daniel Melchor Aguilar, ganadora del premio Arturo Rosenblueth en el 2002. Otra contribución de gran interés fue la extensión de los conocidos teoremas de Nyquist finito y el de inclusión finita al caso de cuasipolinomios para el análisis de familias politópicas e intervalo, el cual culminó con el paquete tipo "toolbox" FITROBUST, el cual es amigable al usuario, y que fuera desarrollado en el marco de la tesis de Joaquín Santos Luna.

Se destacan especialmente contribuciones de relevancia teórica a los trabajos seminales de Krasovskii y Repin, donde se busca extender el célebre segundo método de Lyapunov para el análisis de sistemas libres de retardos al caso de sistemas lineales con retardos. Vladimir Kharitonov presentó la construcción de una funcional de Lyapunov-Krasovskii [4] con derivada negativa definida prescrita que, bajo la suposición de estabilidad del sistema, admite una cota cuadrática inferior, garantizando así su positividad. Esta construcción permitió esclarecer conceptos fundamentales como el de matriz de Lyapunov [5] y el de ecuación de Lyapunov para sistemas con retardos.

Vladimir Kharitonov con sus nueve alumnos de doctorado.

La construcción semianalítica y numérica de la matriz de Lyapunov se materializó en el Toolbox MLYAP, producto del trabajo doctoral de Hiram García Lozano.

Estos resultados se extendieron al caso de sistemas de tipo neutral y con retardos distribuidos, lo que dio lugar a aplicaciones como la determinación de cotas de robustez para el caso de parámetros inciertos, así como a la determinación de cotas exponenciales de la respuesta de los sistemas (tesis de José Eduardo Velásquez Velásquez) y al diseño de controladores iterativos subóptimos (tesis de Omar Jacobo Santos Santos). Finalmente, las propiedades de la ecuación de Lyapunov condujeron a un novedoso método de análisis de estabilidad de sistemas con retardos (tesis de Gilberto García Ochoa).

Los alumnos de doctorado de Vladimir, quienes trabajan hoy en diversas instituciones de reconocido prestigio del país tales como el **Cinvestav** Unidad Saltillo, el Ipicyt San Luis Potosí, la Universidad Autónoma del Estado de Hidalgo, la Universidad Veracruzana y la Autónoma del Estado de México, entre otras, acudieron el 26 de enero a la emotiva jornada organizada en su honor, sin faltar alguno, para presentar los principales resultados de su trabajo con Vladimir. La nutrida audiencia que asistió al evento –investigadores de diversas instituciones del país y de otros departamentos del **Cinvestav**, colegas del departamento, personal administrativo y de apoyo, ex alumnos y alumnos de ingreso reciente– es muestra de la estima y el aprecio ganado a lo largo de estos once años por sus cualidades humanas, dedicación y excelencia científica. Es indudable que la formación de esta escuela tendrá un impacto positivo en la educación superior nacional, así como en la generación de resultados científicos de calidad.

Le deseamos a Vladimir en su regreso al puesto que ocupa en la Universidad de San Petersburgo, la continuación de su exitosa carrera científica, el reencuentro con sus raíces y el disfrute de las célebres noches blancas de San Petersburgo. Sabemos que en los días más crudos del invierno báltico añorará la calidez del clima de México y de su gente, y deseamos que recuerde que, según dicta la tradición mexicana, el Departamento de Control Automático y el **Cinvestav**, siempre serán su casa. ●

[Referencias]

[1] Kharitonov, V.L. Asymptotic stability of an equilibrium position of a family of systems of differential equations. *Differentsialnye uravneniya*, 14: 2086-2088, 1978.

[2] Gu, K., V. L. Kharitonov y J. Chen. *Stability of Time-Delay Systems*. Birkhauser, 2003.

[3] Kharitonov V.L. y J. Torres-Muñoz. Recent results on the robust stability of multivariate polynomials (invited paper). *IEEE Transactions on Circuits and Systems, I: Fundamental Theory and Applications*, 49 (6): 715-724, 2002.

[4] Kharitonov, V.L. y A. P. Zhabko. Lyapunov-Krasovskii approach to the robust stability analysis of time-delay systems. *Automatica*, 39: 15-20, 2003.

[5] Kharitonov, V.L. Lyapunov matrices for a class of time delay systems. *Systems and Control Letters*, 55: 610-617, 2006.

RESEÑA DEL LIBRO

Cryptographic Algorithms on Reconfigurable Hardware

DE: FRANCISCO RODRÍGUEZ HENRÍQUEZ
NAZAR ABBAS SAQIB
ARTURO DÍAZ PÉREZ
ÇETIN KAYA KOÇ

Miguel Ángel León Chávez

La editorial Springer publicó a fines de 2006 un libro que es resultado de una colaboración internacional para diseñar e implementar eficientemente algoritmos criptográficos en *hardware*. Los autores, hoy dispersos por el mundo, trabajaron alguna vez juntos en Oregon California, EUA y posteriormente en México para poner en nuestras manos el estado del campo del arte en dos tópicos de gran importancia: la criptografía y los dispositivos lógicos programables, en particular los FPGAs *(Field Programmable Gate Array)*.

La criptografía es la ciencia que provee algoritmos, mecanismos y protocolos para mantener comunicaciones seguras; es decir, para verificar la supuesta identidad de un usuario o mensaje (autenticación), para proteger los recursos de la red de comunicaciones (control de acceso) y asegurar la información contra revelaciones (confidencialidad) y manipulaciones (integridad) no autorizadas, así como contra la negación del envío-recepción (no rechazo). Es muy probable que a corto plazo cada bit de información que fluya por una red tenga que ser cifrado y descifrado o firmado y verificado, por lo que todos los dispositivos de comunicación (fijos o móviles) tendrán que implementar estos servicios de seguridad.

Un FPGA es un circuito integrado. Pertenece a la familia de dispositivos lógicos programables y contiene una matriz de bloques lógicos configurables (CLB, por sus siglas en inglés), interconectados por un arreglo de interruptores asimismo configurables. Los CLB pueden ser bloques de memoria, controladores de entrada/salida, multiplicadores, componentes configurables o núcleos programables. El uso de FPGAs permite a los diseñadores de *hardware* implementar y probar prácticamente cualquier circuito digital de manera rápida y barata. Por esa razón se utilizan en aplicaciones como el procesamiento de imágenes, visión por computadora, procesamiento digital de señales, etcétera. Además, los FPGAs ofrecen diferentes beneficios para la implementación de algoritmos criptográficos, como la flexibilidad, y puesto que son reconfigurables, las llaves criptográficas se pueden cambiar sin mucho esfuerzo y sin afectar la eficiencia de la implementación.

La eficiencia merece especial atención por los autores del libro porque los recursos de un FPGA son limitados. En cada uno de los capítulos se hace énfasis en el tiempo, el área y el consumo de potencia para lograr los mejores diseños e implementaciones.

El libro *Cryptographic Algorithms on Reconfigurable Hardware* está organizado en diez capítulos, que se resumen a continuación.

En el capítulo 1 se presenta un resumen del libro, se explican los objetivos y las estrategias seleccionadas para lograrlos, y se proporciona un sumario del material presentado.

Una breve introducción a la criptografía moderna se

MIGUEL ÁNGEL LEÓN CHÁVEZ En el año 2000 se doctoró en Informática en el *Institut Nacional Polytechnique de Lorraine* (Francia). Es Profesor Investigador de la Facultad de Ciencias de la Computación-BUAP. Ha publicado 34 artículos arbitrados en revistas, conferencias nacionales e internacionales sobre calidad de servicio y seguridad en buses de campo (Fieldbus), redes inalámbricas e Internet. Fue editor de FeT'2005, publicado por Elsevier, y miembro del comité de programa de varias conferencias internacionales.
mleon@cs.buap.mx

presenta en el capítulo 2, donde además se discuten algunas aplicaciones criptográficas y la conveniencia de implementarlas en *hardware* reconfigurable.

En el capítulo 3 se presenta una breve introducción a la tecnología de *hardware* reconfigurable, se explica el desarrollo histórico de los FPGAs y se incluye una descripción detallada de los productos de las principales compañías fabricantes de FPGAs, como son Xilinx y Altera. Finalmente, se discuten problemas de diseño, métricas y seguridad en el *hardware* reconfigurable.

La criptografía moderna no podría comprenderse sin una base matemática, por lo que en el capítulo 4 se presentan conceptos útiles para realizar operaciones criptográficas de llave simétrica y pública. Especial atención merecen las operaciones con curvas elípticas, las cuales permiten desarrollar criptosistemas de llave pública con llaves de tamaño pequeño.

En el capítulo 5 se presenta el estado del arte en algoritmos aritméticos para campos finitos de números primos y se discuten diferentes alternativas de diseño en *hardware* de operaciones como suma, suma modular, multiplicación modular, exponenciación modular, etcétera. Al final del capítulo se presenta un análisis comparativo de los trabajos más significativos reportados en la literatura.

El estado del arte en algoritmos aritméticos para campos finitos binarios, también llamados campos finitos de Galois, $GF(2^m)$, se presenta en el capítulo 6. Al final de cada sección se realiza un análisis de la complejidad en tiempo y espacio de los algoritmos más significativos reportados en la literatura sobre la multiplicación, raíces, raíz cuadrada, inversión y reducción.

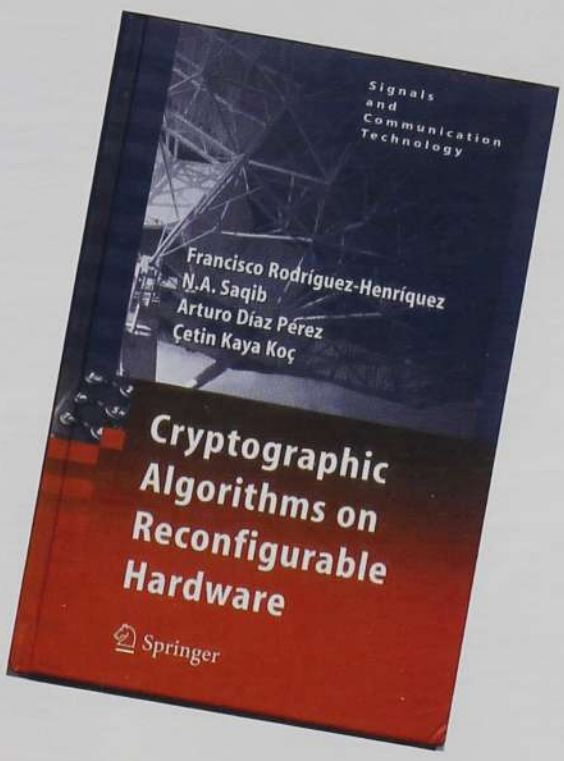
Con el capítulo 7 se introduce al lector en el funcionamiento de las funciones Hash y se discuten aspectos importantes de su implementación en *hardware*. Además, se describe paso a paso la función Hash MD5, para que el lector comprenda las operaciones lógicas y matemáticas involucradas en su funcionamiento y sirva de base para comprender la familia más reciente de funciones Hash SHA2. Al final de cada sección se presenta un análisis de la complejidad de los trabajos publicados.

Guías generales para la implementación eficiente en *hardware* reconfigurable de cifradores por bloque se presentan en el capítulo 8. Se identifican primitivas básicas y se analizan técnicas de diseño útiles, mismas que son aplicadas al Estándar de Cifrado de Datos (DES, *Data Encryption Standard*), y se produce un núcleo compacto de DES. Por último se presenta un resumen de los diseños de DES publicados en la literatura, clasificados por los autores como rápidos, compactos o eficientes.

A lo largo del capítulo 9 se discuten los diseños de las arquitecturas del Estándar Avanzado de Cifrado (AES, *Advanced Encryption Standard*). El primer factor a considerar en la implementación de AES es la aplicación, por ejemplo, la TV de alta definición (HDTV, *High Definition TV*) y la video conferencia requieren alto rendimiento especificado en gigabits por segundo (Gbps), mientras que aplicaciones que se ejecutan en dispositivos móviles ligeros PDA *Personal Digital Assistant* requieren bajo rendimiento o incluso implementaciones compactas RFI, *Radio Frequency Identifiers*. El capítulo concluye con la presentación de implementaciones de AES, optimizadas para ofrecer alto rendimiento, compactas o portables.

Diferentes algoritmos para realizar la multiplicación escalar sobre curvas elípticas y su correspondiente implementación en *hardware* son presentados en el capítulo final. Los autores aplican estrategias paralelas para realizar operaciones aritméticas con curvas elípticas y producir implementaciones muy rápidas. Finalmente, se presenta una comparación de los trabajos publicados en los últimos diez años sobre multiplicación escalar.

Bienvenido sea *Cryptographic Algorithms on Reconfigurable Hardware* porque une dos áreas importantes de la computación moderna, y felicidades a los autores por haber reflejado en el libro su conocimiento, experiencia y arte de diseño. Estoy seguro que este libro contribuirá en la formación de profesionistas mejor capacitados. ●



Noticias Cinvestav

Nombramientos

SECRETARIOS
Dr. Arnulfo Albores Medina
Secretario Académico

Dr. Marco Antonio Meraz Ríos
Secretario de Planeación

JEFES DE DEPARTAMENTO
Dr. Isidoro Gitler Goldwain
Matemáticas

Dr. Isaac Hernández Calderón
Física

Dr. Alexander Poznyak Gorbatch
Control Automático

Dra. Ma. del Jesús Rosales Hoz
Química

Dra. Patricia Talamás Rohana
Patología Experimental

FELLOW DE LA AMERICAN ASSOCIATION FOR THE ADVANCEMENT OF SCIENCE (AAAS),
Nombramiento otorgado al Dr. Jean Philippe Vielle Calzada por haber descubierto que la actividad transcripcional de los genomas parentales no es equivalente en las plantas.

PRIMER LUGAR DEL 19º PREMIO LOLA E IGO FLISSER-PUIS
Obtenido por el Dr. Juan Daniel Díaz Valencia con la tesis de doctorado: *Detección de la interacción de la proteína EhABP-120 de* Entamoeba histolytica *con lípidos y su posible efecto sobre la movilidad del parásito*, bajo la asesoría del Dr. Miguel Ángel Vargas Mejía del Departamento de Biomedicina Molecular.

MENCIÓN HONORÍFICA EN EL 19º PREMIO LOLA E IGO FLISSER-PUIS
A la M. en C. Nidia Maribel León Sicarios por su trabajo: *Caracterización del sistema de adquisición del Hierro (Fe) a partir de la holoLactoferrina por* Entamoeba histolytica *y del mecanismo amebicida de la apoLactoferrina.*

GRADUATE STUDENT TRAVEL SUPPORT
Premio ganado por la M. en C. Laura Arreola Mendoza por su trabajo: *Low doses of dichromate alter paracellular and transcellular transport along the rat nephron*, presentado en el 46º Congreso Anual de la Sociedad de Toxicología de Estados Unidos. Sus tutores, la Dra. Ma. de la Luz del Razo Jiménez, de la Sección Externa de Toxicología, y el Dr. José Luis Reyes Sánchez, del Departamento de Fisiología, Biofísica y Neurociencias.

GRADUATE STUDENT TRAVEL SUPPORT
Distinción lograda por la M. en C. Ana Belém Piña Guzmán con su trabajo: *In vivo methyl-parathion exposure impairs male fertilizing ability in mice*, presentado en el 46º Congreso Anual de la Sociedad de Toxicología de Estados Unidos, bajo la tutoría de la Dra. María Betzabet Quintanilla Vega, de la Sección Externa de Toxicología.

RECONOCIMIENTO DEL CONSEJO DIRECTIVO DEL INSTITUTO DE LAS MUJERES IRAPUATENSES
A la Dra. Gabriela Olmedo Álvarez, en el marco conmemorativo del Día Internacional de las Mujeres, por su destacada labor en investigación y divulgación de la ciencia.

YOUNG SCIENTIST AWARD 2006
Premio otorgado al Dr. Roberto Flores Moreno por haber logrado la mejor tesis de doctorado del Departamento de Química con el trabajo: *Derivadas analíticas en métodos LCGTO-DFT empleando pseudos-potenciales y funciones auxiliares*. Esta distinción es patrocinada por el Profesor Heinrich Nöth de la Universidad Ludwig+Maximiliano de Munich, Alemania.

PREMIO TRIESTE SCIENCE PRIZE
Otorgado al Dr. Luis Rafael Herrera Estrella, por la TWAS e ILLYCAFFE como reconocimiento a la presencia internacional de científicos de los países en desarrollo.

GALARDÓN "MADRE TIERRA, FRESA SOL"
Al Dr. Luis Rafael Herrera Estrella. Distinción que otorga el Consejo Expo-fresas de Irapuato a personas sobresalientes en las artes y/o las ciencias.

PREMIO CANIFARMA VETERINARIA 2007
Al Dr. Miguel Ángel Gómez Lim.

PRIMER LUGAR EN EL CONCURSO PREMIOS A LA INNOVACIÓN EN SALUD Y ALIMENTACIÓN
Otorgado al Dr. Miguel Ángel Gómez Lim en la categoría de vacunas, organizado por Merck Sharp & Dohme (MSD-México).

DESIGNACIÓN COMO "SINALOENSE EJEMPLAR"
Al Dr. Octavio Paredes López por el Consejo Pro Sinaloenses Ejemplares en el Mundo.

BEST STUDENT PAPER AWARD
Reconocimiento dado al M. en C. Alfredo Ortega Clemente en el 9th Internacional in Situ and On-Site Bioremediation Symposium, por el trabajo: *Comparison of two types of fungal bioreactors with inmmobilized Trametes versicolor for post-treated weak black liquor from kraft pulp mills"*. Bajo la dirección de la Dra. Josefina Barrera Cortés y el Dr. Héctor Poggi Varaldo, investigadores del Departamento de Biotecnología y Bioingeniería.

PREMIO WEIZMANN
Al Dr. Alfredo López Ortega en la categoría de Ciencias Exactas por su tesis: *Comportamiento semi-clásico de campos en espacio-tiempos con horizontes*.

NOMBRAMIENTO COMO MIEMBRO DEL CONSEJO CONSULTIVO INTERINSTITUCIONAL
Al Dr. Rafael Quiroz Estrada para la Asignatura de Formación Cívica y Ética de la Secretaría de Educación Pública.

PRESIDENTE DEL COMITÉ INTERNACIONAL DE BIOÉTICA DE LA UNESCO
Nombramiento otorgado al Dr. Adolfo Martínez Palomo.

PRIMER PREMIO EN LA CATEGORÍA DE CARTEL
A la M. en C. Judith Ramos Jiménez por su trabajo: *Histamine augments β_2-adrenoceptor-induced cyclic AMP accumulation in human prostate cancer cells DU-145 independently of known histamine receptors*, como parte de su tesis de doctorado, bajo la tutela del Dr. Francisco Javier Camacho Arroyo, investigador de la Sección Externa de Farmacología.

NOMBRAMIENTO COMO "INGENIERO DEL AÑO 2007",
Por la IEEE Guadalajara al Dr. José Luis Leyva Montiel por sus méritos profesionales y académicos, así como por el alto impacto social que han alcanzado sus actividades.

La Dra. Emilia Ferreiro Schiavi, investigadora del Departamento de Investigaciones Educativas en los pasados meses obtuvo los siguientes reconocimientos:

Doctorado Honoris Causa, otorgado por la Universidad de la Plata en Argentina.

Homenaje a su trayectoria y obra, organizado por el Centro de Estudios Multidisciplinarios e Investigación en Educación, de la Universidad Nacional de Rosario, Argentina.

Título de **Visitante Ilustre** otorgado por resolución del Honorable Concepto Deliberante de la Ciudad de Rosario, Argenina.

Contribuciones

Las contribuciones para la revista *Cinvestav* deberán enviarse a las oficinas centrales o a la dirección de correo electrónico: msantos@cinvestav.mx

Textos

- Deben entregarse en formato de Word con extensión .doc o .rtf, vía correo electrónico o en CD-ROM.
- Cuando se trate de artículos de investigación; la extensión máxima será de 15 cuartillas, los artículos de difusión tendrán 10 cuartillas y Noticias un aproximado de 50 palabras por nota.
- Si el texto incluye tablas, éstas se entregarán en archivo por separado, en texto corrido y con una impresión adjunta que muestre la forma en que debe quedar la tabla. Además, en el original debe señalarse su ubicación. La indicación también es válida para esquemas y cuadros.
- Todo artículo requiere ilustraciones o fotografías para su inserción (ver imágenes y gráficas), acompañadas de un comentario que las identifique.
- Las notas se incluirán al final del trabajo, antes de la bibliografía o de las referencias debidamente numeradas.
- Todas las siglas y los acrónimos empleados deben venir en su forma desatada (p. ej. Conacyt, Consejo Nacional para la Ciencia y la Tecnología).
- Las referencias deben apegarse a los modelos siguientes:

Libro:

Wiener, Norbert, *Cibernética: o el control y la comunicación en animales y máquinas*, Barcelona, Tusquets, 2003.

Artículo de revista:

Ádem, José, 1991, "Algunas consideraciones sobre la prensa en México", *Avance y Perspectiva*, vol. 10, abril-junio, pp. 168-170.

Se sugiere que las referencias sean cuidadosamente revisadas por los autores y que los títulos de los artículos y los nombres de las publicaciones no se abrevien.

Resumen curricular

Todos los textos deben incluir datos del autor: nombre completo, grado académico, adscripción y cargo que desempeña, teléfono y correo electrónico. El resumen no debe rebasar más de 50 palabras.

Imágenes y gráficas

Deben venir en archivos por separado tipo JPG o TIFF, a 300 dpi de resolución con tamaño de 20 cm de base (como mínimo). Las imágenes tomadas con cámaras digitales deberán tener la resolución máxima.
NO SE ACEPTARÁN IMÁGENES DE INTERNET.

Cinvestav
revista@cinvestav.mx
T/F (55) 50 61 33 71
www.cinvestav.mx/publicaciones
Av. Instituto Politécnico Nacional 2508
San Pedro Zacatenco, C.P. 07360
México, DF, México

[Nota]

En breve aparecerá una versión electrónica de la revista *Cinvestav*, donde los lectores tendrán la oportunidad de contribuir con sus reflexiones acerca de los temas que se abordan en los artículos.

Posgrados Cinvestav

Centro de Investigación y de Estudios Avanzados del Instituto Politécnico Nacional

Excelencia en investigación y posgrado

Ciencias Biológicas y de la Salud

Biología Celular
Maestría: Inscripciones en febrero
Doctorado: Admisiones todo el año

Biomedicina Molecular
Maestría: Inscripciones en marzo y septiembre
Doctorado: Admisiones mayo, junio y noviembre

Bioquímica
Maestría: Inscripciones en junio
Doctorado: Inscripciones abril a junio

Biotecnología y Bioingeniería
Maestría: Admisiones en mayo
Doctorado: Admisiones todo el año

Biotecnología y Bioquímica
(Cinvestav-Guanajuato)
Maestría y Doctorado
Examen de admisión en enero y julio

Neurofarmacología y Terapéutica Experimental (Cinvestav-Sede Sur)
Maestría y Doctorado
Examen de Admisión en junio

Farmacología
Maestría: Entrevistas: junio
Doctorado: Inscripciones todo el año

Neurobiología y Fisiología Celular y Molecular
Maestría: Entrevistas en junio
Doctorado: Inscripciones todo el año

Genética y Biología Molecular
Maestría: solicitudes de mayo y junio
Doctorado: solicitudes en agosto y septiembre

Ingeniería Genética (Cinvestav-Guanajuato)
Maestría: Examen de admisión en julio
Doctorado: Examen de admisión en julio

Patología Experimental
Maestría: Admisiones en junio
Doctorado: Inscripciones todo el año

Ciencias del Mar (Cinvestav-Mérida)
Maestría: Admisiones en junio
Doctorado: Ingreso en septiembre y enero

Toxicología
Maestría: Examen y entrevistas en junio
Doctorado: Inscripciones todo el año

Ciencias Exactas y Naturales

Física
Maestría: Admisiones en mayo
Doctorado: Admisiones todo el año

Física Aplicada (Cinvestav-Mérida)
Especialidades en Física Aplicada, Fisicoquímica y Física Teórica
Maestría: Admisión enero y julio
Doctorado: Admisión todo el año

Matemáticas
Especialidad en Matemáticas básicas y Matemáticas Computacionales
Maestría: Admisiones todo el año
Doctorado: Admisiones todo el año

Química
Doctorado Directo: Admisiones en mayo
Inicio del programa: septiembre

Ciencias Sociales y Humanidades

Ecología Humana (Cinvestav-Mérida)
Maestría: Entrevistas en julio

Educación en Ciencias
(Cinvestav-Monterrey)
Maestría: Exámenes en julio y agosto

Investigaciones Educativas
(Cinvestav-Sede Sur)
Maestría: Inscripciones de febrero a marzo
Doctorado: Inscripciones marzo y abril

Matemática Educativa
Maestría: Exámenes y entrevistas en mayo
Doctorado: Admisión en agosto y noviembre

Tecnología y Ciencias de la Ingeniería

Computación
Maestría y Doctorado
Exámenes de Admisión en julio

Computación (Cinvestav-Tamaulipas)
Maestría y Doctorado
Registro de aspirantes enero a julio

Control Automático
Maestría: Admisiones en julio
Doctorado: Admisiones en agosto y noviembre

Ingeniería y Física Biomédicas
(Cinvestav-Monterrey)
Maestría: Exámenes en julio y agosto

Ingeniería Cerámica (Unidad Saltillo)
Maestría y Doctorado
Recepción de documentos en julio

Ingeniería Eléctrica
(Cinvestav-Guadalajara)
Especialidad en Ciencias de la Computación, Control Automático, Diseño Electrónico, Sistemas Eléctricos de Potencia y Telecomunicaciones
Maestría: Examen de admisión en julio
Doctorado: Abierto todo el año

Ingeniería Eléctrica
Especialidades en Bioelectrónica, Comunicaciones, Electrónica del Estado Sólido y Mecatrónica
Maestría: para fechas contactar al departamento de ingeniería eléctrica: ie@cinvestav.mx
Doctorado: Abierto todo el año

Ingeniería Metalúrgica (Cinvestav-Saltillo)
Maestría y Doctorado
Recepción de documentos en julio

Materiales (Cinvestav-Querétaro)
Maestría: Admisiones en mayo
Doctorado: Examen y entrevista en junio

Robótica, Sistemas Inmersos y Manufactura Moderna (Cinvestav-Saltillo)
Maestría y Doctorado
Inscripciones de abril a julio

www.cinvestav.mx

Cinvestav

Av. Instituto Politécnico Nacional No. 2508, Col. San Pedro Zacatenco, C.P. 07360, México, D.F., Tel. 50 61 38 00.

El Cinvestav en fotos

Cinvestav-Saltillo