



**ALFREDO VIOLA
DEAMBROSIS**

Dr

viola@fing.edu.uy

Instituto de Computación
Facultad de Ingeniería Julio Herrera y Reissig 565 Piso 5
CP 11.300
7114244

SNI

Ciencias Naturales y Exactas / Ciencias de la Computación e Información
Categorización actual: Nivel II (Activo)

Fecha de publicación: 19/09/2018
Última actualización SNI: 19/09/2018

Datos Generales

INSTITUCIÓN PRINCIPAL

Universidad de la República/ Facultad de Ingeniería - UDeLaR / Instituto de Computación / Uruguay

DIRECCIÓN INSTITUCIONAL

Institución: Universidad de la República / Facultad de Ingeniería - UDeLaR / Sector Educación Superior/Público
Dirección: Instituto de Computación - Julio Herrera y Reissig 565 Piso 5 / 11300 / Montevideo, Montevideo, Uruguay
Teléfono: (5982) 711 4244 / 127
Correo electrónico/Sitio Web: viola@fing.edu.uy

Formación

Formación académica

CONCLUIDA

DOCTORADO

(1990 - 1995)

University of Waterloo, Canadá
Título de la disertación/tesis: Ph.D en Matemáticas - Opción Ciencias de la Computación
Tutor/es: James Ian Munro y Patricio Poblete
Obtención del título: 1995
Institución financiadora: National Research Council of Canada, Canadá
Palabras Clave: linear probing hashing Diagonal Poisson Transform
Áreas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Algoritmos - Análisis de Algoritmos - Combinatoria - Teoría de la Información

MAESTRÍA

(1988 - 1989)

University of Waterloo, Canadá
Título de la disertación/tesis: Master of Mathematics
Tutor/es: Gastón Gonnet
Obtención del título: 1989
Institución financiadora: National Research Council of Canada, Canadá
Áreas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Algoritmos

GRADO

(1982 - 1986)

Universidad de la República - Facultad de Ingeniería - UDeLaR, Uruguay
Título de la disertación/tesis: Ingeniero de Sistemas en Computación
Obtención del título: 1986
Áreas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Ingeniería en Computación

Idiomas

Español

Entiende muy bien / Habla muy bien / Lee muy bien / Escribe muy bien

Inglés

Entiende muy bien / Habla muy bien / Lee muy bien / Escribe muy bien

Francés

Entiende bien / Habla regular / Lee bien / Escribe regular

Italiano

Entiende regular / Habla regular / Lee bien / Escribe regular

Portugués

Entiende regular / Habla regular / Lee bien / Escribe regular

Áreas de actuación

CIENCIAS NATURALES Y EXACTAS

Ciencias de la Computación e Información / Ciencias de la Computación / combinatoria

CIENCIAS NATURALES Y EXACTAS

Ciencias de la Computación e Información / Ciencias de la Computación / Teoría de la Información

CIENCIAS NATURALES Y EXACTAS

Ciencias de la Computación e Información / Ciencias de la Computación / criptografía

CIENCIAS NATURALES Y EXACTAS

Ciencias de la Computación e Información / Ciencias de la Computación / Algoritmos - Análisis de Algoritmos

Actuación profesional

SECTOR EDUCACIÓN SUPERIOR/PÚBLICO - UNIVERSIDAD DE LA REPÚBLICA - URUGUAY

Facultad de Ingeniería - UDeLaR

VÍNCULOS CON LA INSTITUCIÓN

Funcionario/Empleado (02/2003 - a la fecha)

Instituto de Computación ,40 horas semanales / Dedicación total
Grado 5. DT. desde mayo 2005.
Escalafón: Docente
Grado: Grado 5
Cargo: Efectivo

Funcionario/Empleado (08/1996 - 02/2003)

Instituto de Computación ,40 horas semanales
Grado 4 INCO
Escalafón: Docente
Grado: Grado 4
Cargo: Efectivo

Funcionario/Empleado (07/1990 - 07/1996)

,40 horas semanales
Escalafón: Docente
Grado: Grado 4

Cargo: Efectivo

Funcionario/Empleado (03/1986 - 06/1990)

Instituto de Computación ,30 horas semanales
Grado 2 INCO. Licencia desde Setiembre de 1988 a Enero de 1996 para cursar estudios de posgrado en Canadá
Escalafón: Docente
Grado: Grado 2
Cargo: Interino

Funcionario/Empleado (08/1986 - 09/1987)

IMERL ,10 horas semanales
Grado 1 IMERL
Escalafón: Docente
Grado: Grado 1
Cargo: Interino

Funcionario/Empleado (03/1982 - 12/1985)

Cátedra de Matemática I - Ciencias Económicas ,12 horas semanales
Grado 1. Facultad de Ciencias Económicas - Matemáticas I
Escalafón: Docente
Grado: Grado 1
Cargo: Interino

ACTIVIDADES

LÍNEAS DE INVESTIGACIÓN

Manejo de información en redes globales (01/2006 - a la fecha)

Colaboración con el grupo de sistemas de información dirigido por la Dra. Regina Motz. Participación y colaboración en proyectos de fin de carrera de Ingeniería en Computación y en proyectos PDT y LACCIR (Microsoft). En estos momentos estoy participando en un proyecto LACCIR llamado JARDIN. Mi trabajo consiste en apoyar dicho proyecto como usuario. Más específicamente la idea consiste en utilizar la información del metasitio de la Comunidad Virtual Metodología e Impacto Social de las Tecnologías de la Información y Comunicación en América (MISTICA), para crear una Comunidad Virtual de Aprendizaje (CVA), usando las herramientas y metodologías desarrolladas en este proyecto. La descripción de MISTICA está hecha en la parte "asesorías técnicas" de este CV. En el corto y mediano plazo, mi idea es ayudar consolidar un ámbito virtual a nivel de la región en donde podamos llevar adelante experiencias exitosas del uso de las TICs para el desarrollo de la región. Desde este punto de vista, estoy realizando un nexo entre metodologías modernas relacionadas con la Web Semántica y expertos sociales relacionados con el uso de las TICs para el desarrollo de la Sociedad de la Información y el Conocimiento. Por otro lado, la idea es integrar también más estudiantes a esta iniciativa, y poder llevar adelante proyectos concretos de impacto tanto nacional como regional. Hace tiempo también que vengo pensando en realizar un curso de la carrera sobre este tema, pero me he visto con poco tiempo para llevarlo adelante. Por otro lado considero muy importante poder llevar adelante trabajo de colaboración conjunta con otros grupos de nuestro instituto, aportando cada uno diversos intereses y puntos de vista para un fin común.

5 horas semanales , Integrante del equipo

Equipo:

Áreas de conocimiento:

Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / almacenamiento y recuperación de información
Ingeniería y Tecnología / Ingeniería Eléctrica, Ingeniería Electrónica e Ingeniería de la Información / Ingeniería de Sistemas y Comunicaciones / Tecnologías de la Comunicación en Información
Ingeniería y Tecnología / Ingeniería Eléctrica, Ingeniería Electrónica e Ingeniería de la Información / Ingeniería de Sistemas y Comunicaciones / Sociedad de la Información y Conocimiento

Análisis de Algoritmos - Combinatoria (01/1997 - a la fecha)

Desarrollo y utilización de herramientas analítico-combinatorias para analizar el comportamiento práctico de algoritmos y la eficiencia de performance de diversas estructuras de datos. Además de dictado de cursos de posgrado, se han conseguido financiamientos de proyectos, publicados trabajos en revistas de primer nivel mundial, colaborado con varias instituciones del exterior y organizado LATIN 2000 (una de las conferencias más importantes del mundo en Teoría de la

Computación). Parte de mis trabajos científicos más relevantes (como la resolución del problema sobre "linear probing hashing with buckets" que estaba en el volumen 3 de la colección "The Art of Computer Programming" de D. Knuth) han sido realizadas en el marco de esta área de investigación. Por otro lado, estas herramientas son muy importantes para realizar trabajos interdisciplinarios, en donde hemos realizado investigación conjunta y propuesto nuevos proyectos científico-tecnológicos en criptografía y teoría de la Información. Uno de los desafíos internacionales más relevantes es formar estudiantes capacitados tanto en herramientas analítico-combinatorias para analizar algoritmos como en Teoría de la Información. Hoy en día, quienes trabajamos en esta frontera, somos especialistas de una u otra área, pero no hemos recibido formación conjunta en nuestros estudios. Esperamos que nuevos proyectos de investigación que hemos presentado, y los cursos específicos tanto en Análisis de Algoritmos como en Teoría de la Información, permitan formar estudiantes tanto a nivel de Maestría como a nivel de Doctorado con conocimientos sólidos en ambas áreas del conocimiento.

10 horas semanales , Coordinador o Responsable

Equipo: A. MARTÍN , F. FERNÁNDEZ

Áreas de conocimiento:

Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / análisis de algoritmos

Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / combinatoria

Teoría de la Información (01/2001 - a la fecha)

Desarrollo de un grupo de investigación sólido y de relevancia internacional en Teoría de la Información, en colaboración con el grupo de Teoría de la Información de los laboratorios HP, California. Cuenta con la colaboración de docentes del Instituto de Ingeniería Eléctrica. Se han dictado cursos de posgrado, organizado visitas, hecho pasantías en los laboratorios HP, orientado estudiantes de grado, maestría y doctorado, financiación y ejecución de proyectos de investigación, y organizado un evento internacional de primer nivel mundial como lo es el IEEE Information Theory Workshop en 2006. Se espera que en 2009 termine el primer doctorado de esta colaboración (Álvaro Martín), y ya se han presentado nuevos proyectos nacionales e internacionales (CSIC, ECOS) con participación conjunta de investigadores de los laboratorios HP, California, y estudiantes de posgrado. Un nuevo paso en esta dirección es la creación de un capítulo Uruguay de Teoría de la Información, que va a permitir consolidar colaboración con ITSOC (la Sociedad Internacional de Teoría de la Información) que luego del éxito de ITW en Uruguay, ha decidido apoyar con 10 mil dolares al futuro capítulo Uruguay para financiar actividades de desarrollo de la Teoría de la Información en el Uruguay.

10 horas semanales , Coordinador o Responsable

Equipo: A. MARTÍN , F. FERNÁNDEZ , N. CARRASCO , M. HERNÁNDEZ

Áreas de conocimiento:

Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Teoría de la Información

Criptografía (03/1998 - a la fecha)

Formar estudiantes de grado y posgrado en temas relacionados con criptografía en particular con aplicaciones a transacciones financieras. Se dirigieron 7 proyectos de grado en esta dirección preparando a estudiantes para realizar un trabajo apropiado en su tarea profesional, con especial énfasis a las telecomunicaciones. Este objetivo (iniciado ya en 1998), junto con todo el trabajo realizado en el área de Teoría de la Información (en colaboración con los laboratorios HP California, iniciado en 2000), apunta a formar recursos humanos capacitados en temas criptográficos y sus aplicaciones a las telecomunicaciones. La idea inicial era formar un grupo interdisciplinario que pudiera realizar además de trabajos de investigación, asesoramiento a empresas públicas como ANTEL. Lamentablemente, debido a muchas circunstancias desafortunadas, este plan se vio truncado por interferencia muy fuerte de autoridades de Facultad y otros grupos en otros lugares de Facultad que pretenden realizar estas tareas sin contar con los antecedentes de nuestro grupo de investigación. Es importante recalcar que no tengo la más mínima intención de integrarme a dichas iniciativas, optando como contrapartida por fortalecer el grupo de investigación, la calidad académica, los contactos internacionales y nuevas áreas de trabajo. En estos momentos estamos iniciando trabajos muy promisorios en relación a Funciones Booleanas y sus aplicaciones criptográficas. Este trabajo es en colaboración con la Universidad de Caen (Francia), en donde hemos presentado un proyecto ECOS, que cuenta además con la participación del Dr. Gadiel Seroussi.. A partir de 2008, hemos presentado dos proyectos internacionales con investigadores de Brasil, Chile, Francia, México y Canadá (STIC-AMSUD, y LACCIR-Microsoft), relacionados con "Estudio, propuesta y diseño de algoritmos criptográficos para sistemas computacionales restringidos en poder de cómputo.". Dos nuevas líneas de colaboración que hemos iniciado en los últimos tiempos están vinculados con el Dr. Joachim von zur Gathen (líder del grupo de Criptografía del Bonn-Aachen International Center for Information Technology y quien ha visitado nuestro instituto en 2007 y 2008) y el Dr. Damien Vergnaud del École Normale Supérieure (ENS) de París

quien va a visitar nuestro instituto en octubre 2008 en "provable cryptography" y vamos a realizar trabajos de investigación conjunta. Esperamos que estas iniciativas puedan fortalecer no sólo la colaboración internacional sino que también integrar nuevos estudiantes tanto de grado como de posgrado al grupo de investigación. Por otro lado estamos empezando a colaborar con el grupo de Seguridad Informática del Instituto de Computación dirigido por el Dr. Gustavo Betarte.

10 horas semanales , Coordinador o Responsable

Equipo: A. MARTÍN , F. FERNÁNDEZ , N. CARRASCO , M. HERNÁNDEZ

Áreas de conocimiento:

Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / criptografía

Bioinformática (01/2006 - a la fecha)

Debido a una enfermedad crónica que tengo, y a un hecho familiar muy doloroso originado por la misma enfermedad, he empezado contactos con diversos grupos (relacionados con neurociencias) del Instituto de Investigaciones Biológicas Clemente Estable para realizar investigación conjunta. Aún no hemos realizado actividades conjuntas de colaboración, pero esperamos que podamos consolidar algún trabajo en 2009, que pueda vincular algún proyecto de grado con estudiantes de informática. Esta es una línea nueva y tentativa de investigación conjunta, que si bien es muy promisorio, aún no hemos logrado concretar ningún proyecto conjunto. Esperamos poder dar avances en esta dirección en 2009.

2 horas semanales , Coordinador o Responsable

Equipo:

Áreas de conocimiento:

Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / bioinformática

PROYECTOS DE INVESTIGACIÓN Y DESARROLLO

Red internacional sobre voto electrónico (01/2015 - a la fecha)

Red de colaboración con científicos chilenos y franceses financiado por el INRIA-Chile.

5 horas semanales

Universidad de Chile , Red internacional sobre voto electrónico

Investigación

Integrante del Equipo

En Marcha

Equipo:

Palabras clave: Voto Electrónico

AleaEnAmSud (Proyecto STIC-AMSUD) (12/2015 - 12/2017)

Proyecto STIC-AMSUD con participación de investigadores de la Universidad de Caen y Paris 7 (Francia) y de la Universidad Nacional General Sarmiento (Argentina).

5 horas semanales

STIC-AMSUD

Investigación

Coordinador o Responsable

En Marcha

Alumnos encargados en el proyecto:

Pregrado:2

Doctorado:1

Financiación:

Agencia Nacional de Investigación e Innovación, Uruguay, Cooperación

Equipo:

Palabras clave: criptografía Combinatoria Análisis dinámico de algoritmos

Áreas de conocimiento:

Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Análisis Dinámico de Algoritmos

Combinatoria Analítica y Aplicaciones (04/2015 - 12/2016)

Proyecto de Investigación CSIC con la participación de 2 estudiantes de grado, 1 estudiante de Maestría y un estudiante interesado en ingresar al doctorado.

10 horas semanales

Universidad de la República , CSIC I+D

Investigación

Coordinador o Responsable

En Marcha

Alumnos encargados en el proyecto:
Pregrado:2
Maestría/Magister:1
Doctorado:1
Equipo: SILVEIRA, A. , FONSECA, S. , ROTNDO, P.
Palabras clave: Combinatoria Analítica

DYNALCO: Advances in Analytic Combinatorics: dynamical combinatorics, and applications to number theory, information theory and cryptography. (01/2013 - 01/2014)

Es un proyecto de investigación científica STIC-AMSUD en colaboración con investigadores de la Universidad de Caen, Francia y la Universidad Nacional General Sarmiento, Argentina.

5 horas semanales

STIC-AMSUD

Desarrollo

Coordinador o Responsable

Concluido

Alumnos encargados en el proyecto:

Pregrado:1

Maestría/Magister:2

Equipo: CARRASCO , FERNÁNDEZ , FONSECA

Palabras clave: Análisis de Algoritmos sistemas dinámicos

Areas de conocimiento:

Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / combinatoria analítica

Boole (07/2010 - 07/2013)

Proyecto ANR frances, con la participación de varios de mis coautores. Una parte importante del proyecto se basó en temas relacionados con mis trabajos en funciones Booleanas. Yo he sido invitado varias veces a participar de reuniones científicas en Francia, como investigador invitado, en el marco de este proyecto. He dado también varias charlas.

1 hora semanal

ANR Project BOOLE; ANR-09-BLAN-0011

Investigación

Otros

Concluido

Financiación:

Institución del exterior, Apoyo financiero

Equipo: VIOLA

Palabras clave: funciones booleanas

Areas de conocimiento:

Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / combinatoria analítica

JARDIN: Just an Assistant foR Instructional DesigN (09/2008 - 10/2012)

Proyecto financiado por LACCIR (red latinoamericana impulsada por Microsoft), dirigido por Regina Motz (Universidad de la República, Uruguay) y con participación de miembros de 6 países.

2 horas semanales

Investigación

Integrante del Equipo

En Marcha

Alumnos encargados en el proyecto:

Pregrado:2

Maestría/Magister:1

Financiación:

Institución del exterior, Apoyo financiero

Equipo: R. MOTZ (Responsable)

Estudio cuantitativo de clases de estructuras combinatorias y sus aplicaciones en criptografía y Teoría de la Información (02/2009 - 02/2012)

Programa ECOS de cooperación francesa con la Universidad de París XIII y la Universidad de Caen

5 horas semanales

ECOS

Investigación

Coordinador o Responsable

En Marcha

Alumnos encargados en el proyecto:

Pregrado:1

Maestría/Magister:1

Equipo: N. CARRASCO , M. HERNÁNDEZ , G. SEROUSSI , F. BASSINO , J. CLÉMENT , B. VALLÉE

Palabras clave: funciones booleanas Teoría de la Información criptografía Combinatoria

Areas de conocimiento:

Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / criptografía

Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / combinatoria

FMCrypto: Formal Methods for Cryptographically Secure Distributed Computations (04/2009 - 06/2011)

Programa de cooperación STIC-AMSUD con investigadores de Francia, Brasil y Chile. The overall goal is to investigate complexity-based cryptography from two different angles. First we intend to apply formal methods to security complexity-based cryptographic definitions to give raise to practical and robust notions of security as well as corresponding verification techniques. In particular, we focus on defining anonymous communication against strong adversarial behavior (active attacks by standard computationally bounded adversaries), and cryptographic-based compilation of decentralized access control policies. Secondly, we intend to explore more efficient secure cryptographic primitives implementations. In particular, we intend to achieve fast, and side-channel-attack resistant implementations of traditional primitives, such as those related to asymmetric methods based on factorization and discrete logarithm, but also the more recent pairing-based primitives and those primitives arising from the study of the so-called post-quantum cryptographic schemes, based on coding and lattice theory. Such faster implementations often arise from deeper studies of the underlying theory thus requiring formal proof of their correctness and security.

5 horas semanales

STIC-AMSUD

Investigación

Integrante del Equipo

Concluido

Alumnos encargados en el proyecto:

Pregrado:1

Maestría/Magister:1

Equipo: M. HERNÁNDEZ , G. BETARTE , C. LUNA , F. ZIPITRÍA , T. REZK (Responsable) , R. DAHAB , A. HEVIA

Palabras clave: criptografía seguridad de la información

Areas de conocimiento:

Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / criptografía

Análisis de Funciones Booleanas y sus Aplicaciones a la Criptografía (04/2009 - 06/2011)

Proyecto de Investigación CSIC en conjunto con investigadores de las Universidades de Caen y Paris XIII (Francia)

10 horas semanales

CSIC

Investigación

Coordinador o Responsable

Concluido

Alumnos encargados en el proyecto:

Pregrado:1

Maestría/Magister:1

Financiación:

Comisión Sectorial de Investigación Científica - UDeLaR, Uruguay, Apoyo financiero

Equipo: N. CARRASCO , M. HERNÁNDEZ , G. SEROUSSI , F. BASSINO , J. CLÉMENT

Palabras clave: funciones booleanas criptografía

Areas de conocimiento:

Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / combinatoria

Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / criptografía

Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Teoría de la Información

Codigos libres de prefijos óptimos con alfabetos infinitos y su uso en algoritmos eficientes de compresión (03/2006 - 05/2008)

Proyecto PDT, con participación de investigadores de Francia y de los laboratorios HP, California

10 horas semanales
Investigación
Coordinador o Responsable
Concluido
Alumnos encargados en el proyecto:
Maestría/Magister:1
Equipo: F. FERNÁNDEZ , G. SEROUSSI , F. BASSINO , J. CLÉMENT , A. VIOLA (Responsable)

Estudio de Modelos para procesos estocásticos de memoria finita (03/2005 - 03/2007)

Proyecto CSIC con colaboración de investigadores de los laboratorios HP en California.
10 horas semanales
Desarrollo
Coordinador o Responsable
Concluido
Alumnos encargados en el proyecto:
Doctorado:1
Financiación:
Comisión Sectorial de Investigación Científica - UDeLaR, Uruguay, Apoyo financiero
Equipo: G. SEROUSSI , M WEINBERGER

Diseño, análisis e implementación de diversos algoritmos de almacenamiento, búsqueda y recuperación de información (03/2002 - 03/2004)

Proyecto con colaboración de investigadores de Canadá y España.
10 horas semanales
Desarrollo
Coordinador o Responsable
Concluido
Alumnos encargados en el proyecto:
Pregrado:1
Financiación:
Comisión Sectorial de Investigación Científica - UDeLaR, Uruguay, Apoyo financiero
Equipo: D. PANARIO , C. MARTÍNEZ

Desarrollo de métodos matemáticos para analizar algoritmos y su aplicación al análisis de algoritmos criptográficos (03/2000 - 03/2002)

Proyecto en colaboración con investigadores de Chile y de Canadá.
10 horas semanales
Investigación
Concluido
Alumnos encargados en el proyecto:
Pregrado:4
Financiación:
Comisión Sectorial de Investigación Científica - UDeLaR, Uruguay, Apoyo financiero
Equipo: D. PANARIO , P. POBLETE

Manejo de información en redes globales (03/1997 - 03/1999)

Fondo Clemente Estable
10 horas semanales
Desarrollo
Coordinador o Responsable
Concluido
Alumnos encargados en el proyecto:
Pregrado:8
Equipo:

DOCENCIA

Doctorado en Informática (UDELAR-PEDECIBA) (01/1997 - a la fecha)

Doctorado

Asignaturas:
Análisis de Algoritmos, 4 horas, Teórico-Práctico
Teoría de Códigos, 4 horas, Teórico-Práctico
Criptografía, 4 horas, Teórico-Práctico

Maestría en Informática (UDELAR-PEDECIBA) (01/1997 - a la fecha)

Maestría

Asignaturas:

Análisis de Algoritmos, 4 horas, Teórico-Práctico

Criptografía, 4 horas, Teórico-Práctico

Teoría de Códigos, 4 horas, Teórico-Práctico

Ingeniería en Computación (02/2013 - a la fecha)

Grado

Responsable

Asignaturas:

Teoría de la Computación, 12 horas, Teórico-Práctico

Áreas de conocimiento:

Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación /

Ingeniería en Computación (02/2013 - a la fecha)

Grado

Responsable

Asignaturas:

Combinatoria Analítica, 15 horas, Teórico-Práctico

Áreas de conocimiento:

Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación /

Ingeniería en Computación (06/2015 - a la fecha)

Grado

Asistente

Asignaturas:

Programación 3, 5 horas, Teórico

Maestría en Seguridad Informática (09/2012 - a la fecha)

Maestría

Responsable

Asignaturas:

Fundamentos de Criptografía, 18 horas, Teórico-Práctico

Áreas de conocimiento:

Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación /

Ingeniería en Computación (01/1997 - 12/2002)

Grado

Asignaturas:

Programación 3, 6 horas, Teórico-Práctico

Ingeniería en Computación (03/1986 - 06/1988)

Grado

Asignaturas:

Programación III (Plan 85), 6 horas, Teórico-Práctico

Programación II (Plan 85), 6 horas, Teórico-Práctico

Ingeniería Eléctrica (01/1987 - 06/1988)

Grado

Asignaturas:

Ayudante del curso de Probabilidad y Estadística, 6 horas, Práctico

EXTENSIÓN

Miembro del EDT del proyecto MISTICA, orientado a fortalecer el impacto del uso de las Tecnologías de la Información al desarrollo de América Latina y el Caribe (Sede en República Dominicana) (02/2005 - a la fecha)

5 horas

(06/2010 - a la fecha)

PEDECIBA/Plan Ceibal

3 horas

Áreas de conocimiento:

Ciencias Naturales y Exactas / Otras Ciencias Naturales / Otras Ciencias Naturales / Divulgación científica de todas las áreas del Pedeciba

Asesoramiento al Gobierno Nacional en temas relacionados con comercio electrónico (06/2001 - 06/2004)

2 horas

Asesoramiento al Parlamento Nacional en relación a leyes sobre comercio electrónico (colaboración con Facultad de Derecho) (03/2000 - 06/2002)

5 horas

GESTIÓN ACADÉMICA

Director del grupo de investigación de Algoritmos y Análisis de Algoritmos (01/1997 - a la fecha)

Gestión de la Investigación

Miembro suplente de la Comisión de Instituto (11/2014 - a la fecha)

Facultad de Ingeniería, Instituto de Computación

Participación en cogobierno

Miembro de la Comisión de Planes de Estudio del Claustro (11/2014 - a la fecha)

Gestión de la Enseñanza

Miembro suplente de comisión de instituto de computación (02/2015 - a la fecha)

Participación en cogobierno

Áreas de conocimiento:

Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Análisis Dinámico de Algoritmos

Miembro Alternativo de la Comisión Académica de Posgrado de la Facultad de Ingeniería (08/2005 - 09/2014)

Gestión de la Investigación

Consejero Titular de Facultad de Ingeniería (09/2006 - 06/2014)

Participación en cogobierno

Miembro del Consejo Académico del Instituto de Computación (03/2004 - 07/2008)

Participación en consejos y comisiones

Miembro de la Subcomisión Académica de Posgrado de Ingeniería en Computación (07/1997 - 07/2008)

Gestión de la Investigación

Miembro de la directiva de ADFI (09/2004 - 09/2006)

Participación en cogobierno

Miembro Titular del Claustro de la Facultad de Ingeniería (09/2000 - 09/2004)

Participación en cogobierno

Miembro de la Comisión de Posgrado del Claustro de la Facultad de Ingeniería (09/2000 - 09/2004)

Participación en cogobierno

Ejercicio de dirección del Instituto de Computación en ausencia del director Raúl Ruggia. (03/2000 - 03/2001)

Participación en cogobierno

SECTOR EDUCACIÓN SUPERIOR/PÚBLICO - PROGRAMA DE DESARROLLO DE LAS CIENCIAS BÁSICAS - URUGUAY

VÍNCULOS CON LA INSTITUCIÓN

Colaborador (03/2008 - a la fecha)

Investigador Honorario Grado 5 ,40 horas semanales
Area Informática

Colaborador (03/2001 - 03/2008)

Investigador Honorario Grado 4 ,40 horas semanales
Area de Inforática

Colaborador (03/1996 - 03/2001)

Investigador Honorario Grado 3 ,40 horas semanales
Area de Informática

ACTIVIDADES

GESTIÓN ACADÉMICA

Miembro del Consejo Científico del área de Informática (03/1999 - a la fecha)

Gestión de la Investigación

Delegado de los investigadores a la Comisión Directiva del Pedeciba. (03/2009 - 03/2011)

Participación en consejos y comisiones

Coordinador del Area de Informática del Pedeciba (03/2006 - 12/2007)

Gestión de la Investigación

Miembro de la Comisión de Posgrado del Area de Informática (07/1997 - 07/2007)

Gestión de la Investigación

Coordinador Titular y luego Coordinador Alterno del Pedeciba Informática (03/2001 - 03/2003)

Gestión de la Investigación

SECTOR EXTRANJERO/INTERNACIONAL/OTROS - FRANCIA

Universite de Caen

VÍNCULOS CON LA INSTITUCIÓN

Profesor visitante (07/2017 - 07/2017)

,40 horas semanales

Profesor visitante (06/2015 - 06/2015)

,40 horas semanales

Profesor visitante (06/2014 - 06/2014)

,40 horas semanales

Profesor visitante (06/2013 - 06/2013)

,40 horas semanales
Visita científica en el marco de un proyecto STIC-AMSUD

Profesor visitante (06/2010 - 07/2010)

,40 horas semanales

Profesor visitante (07/2009 - 07/2009)

,40 horas semanales

Profesor visitante (06/2008 - 07/2008)

,40 horas semanales
Departamento de Computación

Profesor visitante (06/2007 - 06/2007)

,40 horas semanales
Departamento de Computación

SECTOR EXTRANJERO/INTERNACIONAL/OTROS - FRANCIA

Université de Paris VI (Pierre et Marie Curie), U.P.VI

VÍNCULOS CON LA INSTITUCIÓN

Profesor visitante (06/2017 - 06/2017)

,40 horas semanales

Profesor visitante (05/2010 - 05/2010)

,40 horas semanales
Invitado por la Dra. Michèle Soria para realizar actividades de investigación conjunta. Esta visita es en colaboración también con la Universidad de París XIII.

SECTOR EXTRANJERO/INTERNACIONAL/OTROS - CHILE

Universidad de Chile

VÍNCULOS CON LA INSTITUCIÓN

Profesor visitante (11/2016 - 11/2016)

,40 horas semanales
Visita científica a Patricio Poblete y Alejandro Hevia

Profesor visitante (12/2012 - 12/2012)

,40 horas semanales

Profesor visitante (12/2009 - 12/2009)

,40 horas semanales
Visita de investigación conjunta con Alejandro Hevia por proyecto STIC - AMSUD

Profesor visitante (12/2007 - 12/2007)

,40 horas semanales
NIC Chile

Profesor visitante (12/2006 - 12/2006)

,40 horas semanales
NIC Chile

Profesor visitante (12/2000 - 12/2000)

,40 horas semanales
Departamento de Ciencias de la Computación

Profesor visitante (12/1999 - 12/1999)

,40 horas semanales
Departamento de Ciencias de la Computación

Profesor visitante (12/1998 - 12/1998)

,40 horas semanales
Departamento de Ciencias de la Computación

Profesor visitante (12/1997 - 12/1997)

,40 horas semanales
Departamento de Ciencias de la Computación

Profesor visitante (12/1996 - 12/1996)

,40 horas semanales
Departamento de Ciencias de la Computación

SECTOR EXTRANJERO/INTERNACIONAL/ENSEÑANZA SUPERIOR - CANADÁ

University of Waterloo

VÍNCULOS CON LA INSTITUCIÓN

Profesor visitante (07/2015 - 07/2015)

,40 horas semanales

Profesor visitante (06/2001 - 06/2001)

,40 horas semanales
Departamento de Computación

Profesor visitante (05/1997 - 06/1997)

,40 horas semanales
Departamento de Computación

Profesor visitante (09/1996 - 09/1996)

,40 horas semanales
Departamento de Computación

Funcionario/Empleado (01/1989 - 07/1995)

Teacher Assistant ,5 horas semanales

SECTOR EXTRANJERO/INTERNACIONAL/ENSEÑANZA SUPERIOR - FRANCIA

Universite de Paris VII

VÍNCULOS CON LA INSTITUCIÓN

Profesor visitante (06/2015 - 06/2015)

,40 horas semanales

SECTOR EXTRANJERO/INTERNACIONAL/OTROS - ESPAÑA

Universidad Politécnica de Catalunya*

VÍNCULOS CON LA INSTITUCIÓN

Profesor visitante (05/2015 - 06/2015)

,40 horas semanales

Profesor visitante (06/2014 - 06/2014)

,40 horas semanales

Profesor visitante (05/2013 - 06/2013)

,40 horas semanales

Profesor visitante (09/2011 - 08/2012)

Año sabàtico ,40 horas semanales
Usufructuo de año sabàtico

Profesor visitante (06/2009 - 06/2009)

,40 horas semanales

Dictado de un curso de maestría y doctorado en Teoría de Códigos

Profesor visitante (07/2008 - 07/2008)

,40 horas semanales

Departamento de Lenguajes y Sistemas Informáticos

Profesor visitante (04/2004 - 04/2004)

,40 horas semanales

Departamento de Lenguajes y Sistemas Informáticos

Profesor visitante (07/2001 - 07/2001)

,40 horas semanales

Departamento de Lenguajes y Sistemas Informáticos

Profesor visitante (11/2000 - 11/2000)

,40 horas semanales

Departamento de Lenguajes y Sistemas Informáticos

Profesor visitante (07/1997 - 07/1997)

,40 horas semanales

Departamento de Lenguajes y Sistemas Informáticos

ACTIVIDADES

DOCENCIA

(07/2001 - 07/2011)

Doctorado

Invitado

Asignaturas:

Análisis de algoritmos de ordenación y búsqueda, 6 horas, Teórico-Práctico

(06/2009 - 06/2009)

Doctorado

Asignaturas:

Introducción a la Teoría de Códigos, 6 horas, Teórico-Práctico

(07/2008 - 07/2008)

Doctorado
Invitado
Asignaturas:
Introducción a la Teoría de Códigos, 6 horas, Teórico-Práctico

SECTOR EXTRANJERO/INTERNACIONAL/ENSEÑANZA SUPERIOR - FRANCIA

Universite de Paris XIII (Paris-Nord)

VÍNCULOS CON LA INSTITUCIÓN

Colaborador (11/2003 - 11/2010)

Profesor Asociado ,1 hora semanal
Colaboración con el Dr. Vlady Ravelomanana y la Dra. Frédérique Bassino. Visitas periódicas a la Universidad cada 2 años.

Profesor visitante (05/2010 - 05/2010)

,40 horas semanales
Investigación conjunta con la Dr. Frédérique Bassino

Profesor visitante (05/2006 - 06/2006)

,40 horas semanales
Laboratorio de Informática (LIPN)

Profesor visitante (06/2003 - 11/2003)

Poste Rouge CNRS ,40 horas semanales / Dedicación total
Laboratorio de Informática (LIPN)

SECTOR EXTRANJERO/INTERNACIONAL/OTROS - ALEMANIA

Universitat Bonn

VÍNCULOS CON LA INSTITUCIÓN

Profesor visitante (06/2010 - 06/2010)

,40 horas semanales
Visita de 1 semana al director del grupo de Computer Security, Dr. Joachim von zur Gathen

Profesor visitante (07/2007 - 07/2007)

,20 horas semanales
Visita al Dr. Joachim von zur Gathen, director del grupo de Criptografía del Bonn-Aachen International Center for Information Technology.

SECTOR EXTRANJERO/INTERNACIONAL/OTROS - CANADÁ

Carleton University

VÍNCULOS CON LA INSTITUCIÓN

Profesor visitante (05/2009 - 05/2009)

,40 horas semanales
Investigación conjunta y participación en dos eventos científicos

Profesor visitante (04/2004 - 04/2004)

,40 horas semanales
Departamento de Matemáticas

Profesor visitante (07/2002 - 07/2002)

,40 horas semanales
Departamento de Matemáticas

Profesor visitante (06/2001 - 06/2001)

,40 horas semanales
Departamento de Matemáticas

SECTOR EXTRANJERO/INTERNACIONAL/OTROS - BRASIL

Universidad Estadual de Campinas

VÍNCULOS CON LA INSTITUCIÓN

Profesor visitante (05/2009 - 05/2009)

,40 horas semanales
Visita al profesor Ricardo Dahab por proyecto STIC-AMSUD

SECTOR EXTRANJERO/INTERNACIONAL/OTROS - FRANCIA

Université de Marne la Vallée

VÍNCULOS CON LA INSTITUCIÓN

Profesor visitante (07/2008 - 07/2008)

,40 horas semanales
Instituto Gaspard Monge

Profesor visitante (07/2007 - 07/2007)

,40 horas semanales
Instituto Gaspard Monge

Profesor visitante (05/2005 - 06/2005)

,40 horas semanales
Instituto Gaspard Monge

SECTOR EXTRANJERO/INTERNACIONAL/OTROS - FRANCIA

Institut National de Recherche en Informatique et Automatique

VÍNCULOS CON LA INSTITUCIÓN

Profesor visitante (06/2007 - 06/2007)

,40 horas semanales
INRIA Rocquencourt; Grupo ALGO. Visita al Dr. Philippe Flajolet

Profesor visitante (06/2002 - 06/2002)

,40 horas semanales
INRIA Rocquencourt; Grupo ALGO, Visita al Dr. Philippe Flajolet.

SECTOR EXTRANJERO/INTERNACIONAL/OTROS - ESTADOS UNIDOS

Hewlett-Packard Laboratories

VÍNCULOS CON LA INSTITUCIÓN

Profesor visitante (01/2007 - 01/2007)

,40 horas semanales
Grupo de Teoría de la Información

Profesor visitante (06/2004 - 06/2004)

,40 horas semanales
Grupo de Teoría de la Información

Profesor visitante (01/2002 - 01/2002)

,40 horas semanales
Grupo de Teoría de la Información

CARGA HORARIA

Carga horaria de docencia: 10 horas
Carga horaria de investigación: 15 horas
Carga horaria de formación RRHH: 10 horas
Carga horaria de extensión: 5 horas
Carga horaria de gestión: 20 horas

Producción científica/tecnológica

Mis áreas de investigación principal son análisis de algoritmos y combinatoria, aunque en los últimos años he publicado en el área de Teoría de la Información, especialmente en el área de codificación y criptografía.

Dada la dificultad para realizar investigación científica en Uruguay, decidí jerarquizar la calidad y el impacto de mis trabajos sobre la cantidad de los mismos. Por tal motivo decidí presentar menos trabajos, pero jerarquizando su impacto. Mis trabajos de investigación son citados en varios libros de alta difusión mundial (siendo los de mayor relevancia en sus áreas). Uno de ellos, "The Art of Computer Programming" de D. E. Knuth es el libro más vendido y de mayor impacto en la historia de la computación.

Uno de mis trabajos fundamentales está precisamente relacionado con la resolución de un problema de dificultad 48 (sobre un máximo de 50) de la primera edición del volumen 3 de "The Art of Computer Programming", que generaliza el primer análisis hecho precisamente por D. Knuth y que dio origen tanto al área de investigación de Análisis de Algoritmos, como de la colección "The Art of Computer Programming". Dicha solución es presentada en la segunda edición de dicho volumen 3. Recientemente en 2010 he generalizado este resultado, encontrando resultados distribucionales en donde una componente fundamental es la presentación de una nueva familia de secuencias de números llamada Tuba Numbers, y que ha aparecido en un volumen especial dedicado a los 60 años del Dr. Philippe Flajolet.

En los últimos años he comenzado a trabajar junto con el Dr. Le Bars de la Universidad de Caen (Francia) en el estudio de propiedades combinatorias de funciones booleanas y su impacto en criptografía. Hemos caracterizado completamente a las funciones 1 resilientes, y este trabajo fue presentado en la conferencia más importante del mundo en Teoría de la Información (ISIT) y hay una versión revista en las IEEE Transactions on Information Theory en proceso de evaluación. En estos momentos estamos trabajando en caracterizar a las funciones Bent y funciones con alta inmunidad algebraica. Avances en esta dirección son de importancia fundamental para entender y construir funciones booleanas con aplicaciones a la criptografía.

Considero que parte fundamental de nuestro trabajo en Uruguay es ayudar a crear nuevas áreas de investigación inexistentes en el país y de alto interés estratégico. Al organizar LATIN 2000 en Uruguay, invité al Dr. Gadiel Seroussi, fundador del grupo de Teoría de la Información en los laboratorios H.P, California. Ahi surgió una colaboración junto con Ingeniería Eléctrica y Computación que abarca dictado de cursos en teoría de códigos y codificación de fuentes, orientación de estudiantes de maestría y doctorado, presentación y aprobación de proyectos de investigación, pasantías de estudiantes e investigadores en los laboratorios HP, organización de ITW en Uruguay (Workshop donde vinieron las figuras más relevantes del mundo en Teoría de la Información) y publicaciones de trabajos conjuntos en las mejores revistas y conferencias del mundo. Esperamos que en 2010 se consolide la formación de este grupo interdisciplinario.

Producción bibliográfica

ARTÍCULOS PUBLICADOS

ARBITRADOS

Analysis of Robin Hood and other hashing algorithms under the random probing model, with and without deletions (Completo, 2016)

P. POBLETE , VIOLA, A.
Combinatorics Probability and Computing (E), 2016
Palabras clave: hashing
Areas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / análisis de algoritmos
ISSN: 14692163

A unified approach to linear probing hashing (aceptado en número especial para trabajos seleccionados AofA2014) (Completo, 2016)

SVANTE JANSON , VIOLA, A.
Algorithmica, v.: 75 p.:1 - 58, 2016
Palabras clave: hashing
Areas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / combinatoria analítica
Medio de divulgación: Internet
ISSN: 01784617
Considero que es el mejor trabajo de mi carrera científica.

Scopus' WEB OF SCIENCE"

Optimal prefix codes for pairs of geometrically-distributed random variables (Completo, 2013)

BASSINO, F , CLÉMENT, J , SEROUSSI, G , VIOLA, A.
IEEE Transactions on Information Theory, v.: 59 4 , p.:2375 - 2395, 2013
Palabras clave: Códigos de prefijos óptimos alfabetos infinitos distribución geométrica bidimensional
Areas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Teoría de la Información
Medio de divulgación: Papel
ISSN: 00189448

Scopus' WEB OF SCIENCE"

Enumerative Encoding of first order correlation immune Boolean Functions (Completo, 2013)

N. CARRASCO , LE BARS J.M. , VIOLA, A.
Theoretical Computer Science, v.: 487 p.:23 - 36, 2013
Palabras clave: Resilient Functions Enumerative Coding
Areas de conocimiento:
Ingeniería y Tecnología / Ingeniería Eléctrica, Ingeniería Electrónica e Ingeniería de la Información / Telecomunicaciones / Boolean Functions
ISSN: 03043975

Scopus' WEB OF SCIENCE"

Counting reducible, squareful, and relatively irreducible multivariate polynomials over finite fields (Completo, 2013)

GATHEN J. , ZIEGLER K. , VIOLA, A.
SIAM Journal on Discrete Mathematics, v.: 27 2 , p.:855 - 891, 2013
Areas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / análisis de algoritmos
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / cuerpos finitos
ISSN: 08954801

Scopus' WEB OF SCIENCE"

How to achieve the security of MACs via Randomized Message Preprocessing (en preparación) (Completo, 2011)

D. VERGNAUD , VIOLA, A.

Finite Fields and their Applications, 2011

Palabras clave: polynomials over finite fields

Areas de conocimiento:

Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / criptografía

Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / cuerpos finitos

ISSN: 10715797

Scopus[®] WEB OF SCIENCE[™]

Efficiency of Anonymous Cryptographic Communication with DC Nets (En preparación) (Completo, 2011)

A. HEVIA , P. POBLETE , VIOLA, A.

Theoretical Computer Science, 2011

Palabras clave: DC Nets

Areas de conocimiento:

Ciencias Naturales y Exactas / Matemáticas / Matemática Aplicada / Criptografía

Ciencias Naturales y Exactas / Matemáticas / Matemática Aplicada / Combinatoria

ISSN: 03043975

Scopus[®] WEB OF SCIENCE[™]

Maximal Displacement in Linear Probing Hashing with a Robin Hood Protocol (EN Preparación) (Completo, 2011)

DEVROYE, L, VIOLA, A.

Information Processing Letters, 2011

Palabras clave: linear probing hashing Longest Probe

Areas de conocimiento:

Ciencias Naturales y Exactas / Matemáticas / Matemática Aplicada / Probabilistic Analysis of Algorithms

ISSN: 00200190

Scopus[®] WEB OF SCIENCE[™]

Equivalence classes of boolean functions for first-order correlation (Completo, 2010)

LE BARS, J. M. , VIOLA, A.

IEEE Transactions on Information Theory, v.: 56 3 , p.:1247 - 1261, 2010

Palabras clave: funciones inmunes a la correlación funciones booleanas 1-resilientes

Areas de conocimiento:

Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Funciones booleanas, criptografía

Medio de divulgación: Papel

ISSN: 00189448

Scopus[®] WEB OF SCIENCE[™]

Distributional Analysis of the Parking Problem and Robin Hood Linear Probing Hashing with Buckets - Número especial dedicado a los 60 años de Philippe Flajolet - (Completo, 2010)

VIOLA, A.

Discrete Mathematics and Theoretical Computer Science (DMTCS), v.: 12 2 , p.:307 - 332, 2010

Palabras clave: linear probing hashing with buckets Parking Problem

Areas de conocimiento:

Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / analisis de algoritmos

ISSN: 13658050

www.dmtcs.org/dmtcs-ojs/index.php/dmtcs/article/download/1359/2918

Considero que es el mejor trabajo de mi carrera científica hasta el momento. Número especial dedicado a los 60 años de Philippe Flajolet, miembro de la Academia de Ciencias Francesa, y el líder mundial en el área de Análisis de Algoritmos. En 1998 resolví un problema abierto que aparece en el tercer volumen de la colección "The Art of Computer Programming" de Donald Erwin Knuth. Esta es la colección más vendida y leída en la historia de la Computación. Este problema ("linear probing hashing") fue el primer problema que D. Knuth analizó en 1962 y dio origen a esta colección de libros. Además este análisis es considerado como el punto inicial de la creación del área de investigación Análisis de Algoritmos. En este trabajo, generalizo dicho análisis, dando la distribución completa del costo de búsqueda de un elemento aleatorio (en el libro sólo se pedía por el valor esperado), y además resuelvo dos problemas muy importantes que estaban sin resolver. El primero es la distribución del "Bucket occupancy", y el otro es una solución distribucional del "Parking

Problem with Buckets". Una clave fundamental para resolver estos problemas fue la presentación de una nueva secuencia de números llamada "Tuba Numbers".

Scopus'

Adaptive Sampling Strategies for Quickselect (Completo, 2010)

MARTÍNEZ, C , PANARIO, D , VIOLA, A.

ACM Transactions on Algorithms, v.: 6 3 , 2010

Palabras clave: algoritmos de seleccion

Areas de conocimiento:

Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / analisis de algoritmos

Medio de divulgación: Papel

Lugar de publicación: Articulo 53

ISSN: 15496325

<http://talg.acm.org/>

Scopus' WEB OF SCIENCE"

Exact distribution of individual displacements in linear probing hashing (Completo, 2005)

VIOLA, A.

ACM Transactions on Algorithms, v.: 1 2 , p.:214 - 242, 2005

Palabras clave: linear probing hashing Exact Distribution

Areas de conocimiento:

Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / analisis de algoritmos

Medio de divulgación: Papel

ISSN: 15496325

<http://talg.acm.org/>

On worst case Robin Hood Hashing (Completo, 2004)

DEVROYE, L , MORIN, P , VIOLA, A.

SIAM Journal on Computing, v.: 33 4 , p.:923 - 936, 2004

Palabras clave: Robin Hood Hashing

Areas de conocimiento:

Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / ontologías

Medio de divulgación: Papel

ISSN: 00975397

<http://epubs.siam.org/sam-bin/dbq/article/40337>

Scopus' WEB OF SCIENCE"

Analysis of Rabin's Irreducibility Test for Polynomials over Finite Fields (Completo, 2001)

PANARIO, D , PITTEL, B , RICHMOND, B , VIOLA, A.

Random Structures Algorithms, v.: 19 3-4 , p.:525 - 551, 2001

Palabras clave: polinomios sobre cuerpos finitos

Areas de conocimiento:

Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / analisis de algoritmos

Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / criptografía

Medio de divulgación: Papel

ISSN: 10429832

<http://www3.interscience.wiley.com/cgi-bin/issuetoc?ID=88510505>

Scopus' WEB OF SCIENCE"

Analysis of Linear Probing Hashing with Buckets (Completo, 1998)

VIOLA, A. , POBLETE, P

Algorithmica, v.: 21 1 , p.:37 - 71, 1998

Palabras clave: linear probing hashing with buckets

Areas de conocimiento:

Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / analisis de algoritmos

Medio de divulgación: Papel

ISSN: 01784617

<http://www.informatik.uni-trier.de/~ley/db/journals/algorithmica/algorithmica21.html>

En este trabajo se resuelve un problema abierto de nivel 48 del libro 3 de la colección "The Art of Computer Programming" de D. Knuth. En particular generaliza los resultados del primer análisis hecho por D. Knuth en su vida en 1962 y que dio origen al área de Análisis de Algoritmos y fue su inspiración para iniciar esta famosa colección de volúmenes. Este trabajo además fue el origen de varias correspondencias epistolares y por e-mail (que documento) con D. Knuth que culminaron con el paper "On the Analysis of Linear Probing Hashing" indicado más arriba en conjunto con el paper de D. Knuth "Linear Probing and Graphs" que aparece en el mismo volumen.

Scopus WEB OF SCIENCE™

On the Analysis of Linear Probing Hashing (Completo, 1998)

FLAJOLET, P , POBLETE, P , VIOLA, A.
Algorithmica, v.: 22 4 , p.:490 - 515, 1998

Palabras clave: linear probing hashing

Áreas de conocimiento:

Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / análisis de algoritmos

Medio de divulgación: Papel

ISSN: 01784617

<http://www.informatik.uni-trier.de/~ley/db/journals/algorithmica/algorithmica22.html>

Scopus WEB OF SCIENCE™

The diagonal Poisson transform and its application to the analysis of a hashing scheme (Completo, 1997)

POBLETE, P , VIOLA, A. , MUNRO, I
Random Structures Algorithms, v.: 10 2 , p.:221 - 255, 1997

Palabras clave: linear probing hashing Diagonal Poisson Transform

Áreas de conocimiento:

Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / análisis de algoritmos

Medio de divulgación: Papel

ISSN: 10429832

<http://www3.interscience.wiley.com/cgi-bin/issuetoc?ID=69000567>

Scopus WEB OF SCIENCE™

LIBROS

Selected papers LATIN 2014 (Libro compilado Revista , 2015)

VIOLA, A.

Número de volúmenes: 200

Número de páginas: 300

Edición: ,

Editorial: ,

Tipo de publicación: Investigación

Referado

En prensa

Palabras clave: Teoría de la Computación

Áreas de conocimiento:

Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Teoría de la Computación

Medio de divulgación:

ISSN/ISBN:

Financiación/Cooperación:

Facultad de Ingeniería - UDeLaR / Otra, Uruguay

Proceedings LATIN 2014 (Libro compilado Libro , 2014)

PARDO, A. , VIOLA, A.

Número de volúmenes: 150

Número de páginas: 767

Edición: ,

Editorial: ,

En prensa

Palabras clave: Teoría de la Computación

Áreas de conocimiento:

Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación /

Medio de divulgación:
ISSN/ISBN:

Space-Efficient Data Structures, Streams and Algorithms (papers in honor of J. Ian Munro on the occasion of his 66th birthday) (Libro compilado Libro , 2013)

LÓPEZ-ORTIZ, A. , BRODNIK,A , RAMAN,V , VIOLA, A.

Número de volúmenes: 150

Número de páginas: 362

Edición: , 8066

Editorial: LNCS - SPRINGER,

En prensa

Palabras clave: Algorithms

Areas de conocimiento:

Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación /

Medio de divulgación:

ISSN/ISBN:

Philippe Flajolet's collected works (7 volumes) (Participación , 2013)

VIOLA, A.

Edición: ,

Editorial: ,

Palabras clave: hashing

Areas de conocimiento:

Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / combinatoria analítica

Medio de divulgación:

ISSN/ISBN:

Es la introducción del capítulo sobre hashing en la colección completa de los trabajos de Philippe Flajolet. Philippe Flajolet, miembro de la academia de ciencias francesa, fue el líder de nuestra comunidad científica, y desarrolló los fundamentos del área de Combinatoria Analítica. Falleció en marzo 2011, y se está editando una colección completa de su trabajo científico. Se nos pidió a varios editores que nos encargáramos de presentar ciertos capítulos. A mi me tocó presentar el capítulo sobre hashing, dado que he tenido trabajos conjuntos con Philippe Flajolet.

Capítulos:

Introduction to the chapter «Philippe Flajolet and his contribution to the analysis of hashing problems».

Organizadores: Mark Ward, Robert Sedgewick, Bruno Salvy, Philippe Flajolet, Michele Soria, Brigitte Vallee, Hsien-Kuei Hwang

Página inicial 355, Página final 360

Proceedings LATIN 2000 (Libro compilado Compilación , 2000)

G. H. GONNET , D. PANARIO , VIOLA, A.

Número de volúmenes: 150

Número de páginas: 484

Edición: , 1776

Editorial: LNCS - SPRINGER,

En prensa

Palabras clave: Teoría de la Computación

Areas de conocimiento:

Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación /

Medio de divulgación:

ISSN/ISBN: 3540673067

PUBLICACIÓN DE TRABAJOS PRESENTADOS EN EVENTOS

Beyond series-parallel concurrent systems: the case of arch processes (2018)

Resumen expandido

VIOLA, A. , BODINI, Olivier , DIEN, Matthieu , GENITRINI, Antoine

Evento: Internacional

Descripción: Conference on Analysis of Algorithms 2018

Ciudad: Uppsala

Año del evento: 2018
Publicación arbitrada
<http://math.uu.se/aofa2018>

Analysis of the Continued Logarithm Algorithm (2018)

Resumen expandido
VIOLA, A. , Rotondo, Pablo , Vallée, Brigitte

Evento: Internacional
Descripción: LATIN 2018 (Latin American Theoretical INformatics)
Ciudad: Buenos Aires
Año del evento: 2018
Publicación arbitrada
Palabras clave: continued logarithm dynamical analysis
Areas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación /
Medio de divulgación: Internet
<https://arxiv.org/pdf/1801.10139>
Trabajo en cotutela con el estudiante Pablo Rotondo.

Robin Hood Hashing really has constant average search cost and variance in full tables (2016)

Resumen expandido
P. POBLETE , VIOLA, A.

Evento: Internacional
Descripción: 27th International Conference on Probabilistic, Combinatorial and Asymptotic Methods for the Analysis of Algorithms (AOFA 2016)
Ciudad: Cracovia, Polonia
Año del evento: 2016
Publicación arbitrada
Palabras clave: Robin Hood Hashing
Areas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / análisis de algoritmos
Medio de divulgación: Internet
<https://arxiv.org/submit/1559349>
Financiado por proyecto CSIC: "Combinatoria Analítica y aplicaciones a Criptografía, Comunicaciones y Recuperación de la Información.

Recurrence function on Sturmian words: a probabilistic study (2015)

Resumen expandido
BERTHÉ V. , CESARATTO, E. , ROTNDO, P. , B. VALLÉE , VIOLA, A.

Evento: Internacional
Descripción: Mathematical Foundations of Computer Science
Ciudad: Milán
Año del evento: 2015
Anales/Proceedings:Mathematical Foundations of Computer Science
Publicación arbitrada
Palabras clave: Análisis dinámico de algoritmos
Areas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / combinatoria analítica
Medio de divulgación: Internet
<http://mfcs2015.di.unimi.it/>

A unified approach to linear probing hashing (2014)

Resumen expandido
SVANTE JANSON , VIOLA, A.

Evento: Internacional
Descripción: AofA 2014
Ciudad: París
Año del evento: 2014

Publicación arbitrada
Palabras clave: linear probing hashing
Areas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / combinatoria analítica

Beating the Birthday Paradox in Dining Cryptographer Networks (2014)

Resumen expandido
GARCÍA, P., VAN DE GRAAF, J., A. HEVIA, VIOLA, A.

Evento: Internacional
Descripción: LATINCRYPT 2014
Ciudad: Florianópolis
Año del evento: 2014
Publicación arbitrada
Palabras clave: DC Nets
Areas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / criptografía
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / combinatoria analítica

Counting Distinct Elements in Data Streams: the Random Permutation Viewpoint (2012)

Resumen expandido
HELMI, A., LUMBROSO, J., C. MARTÍNEZ, VIOLA, A.

Evento: Internacional
Descripción: 23rd international meeting on probabilistic, combinatorial and asymptotic methods for the analysis of algorithms (AofA 2012)
Ciudad: Montreal, Canadá
Año del evento: 2012
Palabras clave: data streaming hiring problem distinct elements estimation
Areas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / combinatoria
Ingeniería y Tecnología / Ingeniería Eléctrica, Ingeniería Electrónica e Ingeniería de la Información / Telecomunicaciones / data flow analysis
<http://luc.devroye.org/AofA2012.html>

Enumerative encoding of correlation immune Boolean functions (2011)

Resumen expandido
N. CARRASCO, LE BARS J.M., VIOLA, A.

Evento: Internacional
Descripción: IEEE Information Theory Workshop
Ciudad: Paraty, Brasil
Año del evento: 2011
Publicación arbitrada
Palabras clave: Resilient Boolean Functions Enumerative Encoding
Areas de conocimiento:
Ciencias Naturales y Exactas / Matemáticas / Matemática Aplicada / Teoría de la Información
Ciencias Naturales y Exactas / Matemáticas / Matemática Aplicada / Combinatoria
Medio de divulgación: Internet
<http://edas.info/p10517>

Efficient algorithms for constructing bi-directional context sets (2010)

Resumen expandido
F. FERNÁNDEZ, VIOLA, A., M WEINBERGER

Evento: Internacional
Descripción: IEEE Data Compression Conference
Año del evento: 2010
Palabras clave: context sets
Areas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la

Computación / Estructuras de Datos
Ingeniería y Tecnología / Ingeniería Eléctrica, Ingeniería Electrónica e Ingeniería de la Información /
Telecomunicaciones / Teoría de la Información

Counting reducible, squareful, and relatively irreducible multivariate polynomials over finite fields (2010)

Resumen expandido
GATHEN J., VIOLA, A., ZIEGLER K.

Evento: Internacional
Descripción: LATIN 2010
Ciudad: Oaxaca, Mexico
Año del evento: 2010
Publicación arbitrada
Palabras clave: polinomios sobre cuerpos finitos
Áreas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la
Computación / combinatoria
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la
Computación / cuerpos finitos

Equivalence classes of boolean functions for first-order correlation (2007)

Completo
LE BARS, J. M., VIOLA, A.

Evento: Internacional
Descripción: IEEE International Symposium on Information Theory
Año del evento: 2007
Palabras clave: funciones booleanas 1-resiliente
Áreas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la
Computación / criptografía
Medio de divulgación: Papel

Optimal prefix codes for pairs of geometrically-distributed random variables (2006)

Completo
BASSINO, F, CLÉMENT, J, SEROUSSI, G, VIOLA, A.

Evento: Internacional
Descripción: ISIT - IEEE International Symposium of Information Theory
Año del evento: 2006
Palabras clave: Códigos de prefijos óptimos
Áreas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la
Computación / Teoría de la Información
Medio de divulgación: Papel

Optimal prefix codes for some families of two-dimensional geometric distributions (2006)

Completo
BASSINO, F, CLÉMENT, J, SEROUSSI, G, VIOLA, A.

Evento: Internacional
Descripción: DCC - IEEE Data Compression Conference
Año del evento: 2006
Palabras clave: Códigos de prefijos óptimos
Áreas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la
Computación / Teoría de la Información
Medio de divulgación: Papel

Distributional Analysis of Robin Hood Linear Probing Hashing with Buckets (2005)

Completo
VIOLA, A.

Evento: Internacional

Descripción: First International Conference on Analysis of Algorithms

Año del evento: 2005

Palabras clave: Exact Distribution linear probing hashing with buckets

Areas de conocimiento:

Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / análisis de algoritmos

Medio de divulgación: Papel

<http://www.lsi.upc.es/~aofa05>

Considero que este es mi mejor trabajo académico hasta el momento. En este trabajo, no sólo resuelvo un problema abierto de dificultad 48 (de un máximo de 50) aparecido en la primera edición del volumen 3 de "The Art of Computer Programming" de D. Knuth (el libro más vendido y usado en la historia de la computación) sino que además encuentro una solución más general. Este problema está relacionado con "Linear Probing Hashing", que fue el primer análisis realizado por D. Knuth y que lo inspiró a escribir esta clásica colección de libros. En el problema se pedía hallar el valor esperado del costo de búsqueda de un elemento aleatorio si se inserta en una tabla de hash con buckets de tamaño $b \geq 1$. En este trabajo no solo presento una solución al problema, sino que además hallo toda la distribución de esta variable aleatoria! Parte fundamental de su resolución fue definir la familia de secuencias "Tuba Numbers" que es la secuencia que aparece en "<http://public.research.att.com/~njas/sequences/A124453>". En estos momentos estoy trabajando en una versión revista, que espero presentar en una revista de primer nivel.

Adaptive Sampling Strategies for Quickselect (2004)

Completo

MARTÍNEZ, C , PANARIO, D , VIOLA, A.

Evento: Internacional

Descripción: ACM Symposium on Discrete Algorithms - SODA

Año del evento: 2004

Palabras clave: algoritmos de selección

Areas de conocimiento:

Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / análisis de algoritmos

Medio de divulgación: Papel

Analysis of Quickfind with small subfiles (2002)

Completo

MARTÍNEZ, C , PANARIO, D , VIOLA, A.

Evento: Internacional

Descripción: Colloquium on Mathematics and Computer Science: Algorithms, Trees, Combinatorics and Probabilities

Ciudad: Versailles

Año del evento: 2002

Palabras clave: algoritmos de selección

Areas de conocimiento:

Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / análisis de algoritmos

Medio de divulgación: Papel

The Effect of Deletions on Different Insertion Disciplines for Hash Tables (2001)

Completo

POBLETE, P , VIOLA, A.

Evento: Internacional

Descripción: First Brazilian Symposium on Graphs, Algorithms and Combinatorics - GRACO

Año del evento: 2001

Anales/Proceedings: Electronic Notes in Discrete Mathematics

Volumen: 7

Palabras clave: Hashing Algorithms Deletions

Areas de conocimiento:

Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / análisis de algoritmos

Medio de divulgación: Papel

Average Case Analysis of Rabin's Irreducibility Test Algorithm (1998)

Completo
PANARIO, D., VIOLA, A.

Evento: Internacional
Descripción: Tercer Latin American symposium on Theoretical Informatics
Año del evento: 1998
Anales/Proceedings: Lecture Notes in Computer Science
Volumen: 1380
Página inicial: 1
Página final: 10
Palabras clave: polinomios sobre cuerpos finitos tests de irreducibilidad
Áreas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / análisis de algoritmos
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / criptografía
Medio de divulgación: Papel
<http://www.informatik.uni-trier.de/~ley/db/conf/latin/latin98.html>

Analysis of linear probing hashing with buckets (1996)

Completo
VIOLA, A., POBLETE, P

Evento: Internacional
Descripción: 4th European Symposium on Algorithms
Año del evento: 1996
Anales/Proceedings: Lecture Notes in Computer Science
Volumen: 1136
Página inicial: 221
Página final: 233
Palabras clave: linear probing hashing with buckets
Áreas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / análisis de algoritmos
Medio de divulgación: Papel
<http://www.informatik.uni-trier.de/~ley/db/conf/esa/esa96.html>

Analysis of a Hashing Scheme by a New Transform (1994)

Completo
POBLETE, P., VIOLA, A., MUNRO, I

Evento: Internacional
Descripción: 2nd European Symposium on Algorithms
Año del evento: 1994
Anales/Proceedings: Lecture Notes in Computer Science
Volumen: 855
Página inicial: 94
Página final: 105
Palabras clave: linear probing hashing Transformada Diagonal de Poisson
Áreas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / análisis de algoritmos
Medio de divulgación: Papel

Learning Secondary Structure of Proteins (1994)

Completo
VIOLA, A., LI, M

Evento: Internacional
Descripción: 6th International Conference on Computing and Information
Año del evento: 1994
Palabras clave: estructura secundaria de proteínas
Áreas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / bioinformática
Medio de divulgación: Papel

Producción técnica

TRABAJOS TÉCNICOS

Miembro del Equipo de Transición de la Comunidad Virtual Metodología e Impacto Social de las Tecnologías de la Información y de la Comunicación en América (MISTICA) (2005)

Asesoramiento

VIOLA, A.

Colaborar en la propuesta de reestructura de dicha CV y su viabilidad futura

País: República Dominicana

Idioma: Español

Disponibilidad: Restringida

Duración: 36 meses

Institución financiadora: Sin fines de lucro

Palabras clave: TICs y desarrollo social Sociedad de la Información

Áreas de conocimiento:

Ingeniería y Tecnología / Ingeniería Eléctrica, Ingeniería Electrónica e Ingeniería de la Información /

Ingeniería de Sistemas y Comunicaciones / Tecnologías de la Comunicación en Información

Medio de divulgación: Internet

<http://funredes.org/mistica>

Mi vínculo con MISTICA se originó cuando yo era miembro del SC de Eurolatis, cuando me puse en contacto con el director de la ONG FUNREDES, Daniel Plmienta, quien era miembro del SC por parte de la República Dominicana. MISTICA es un espacio de reflexión - acción sobre el uso de las TICs para el desarrollo social en nuestra región. Parte importante de dicha actividad es la creación de un metaspacio en donde se presentan visiones desde el punto de vista de los actores sociales sobre cómo debe llevarse adelante el uso de las TICs para el desarrollo de la región. También había una mailing list, y se presentaron un conjunto muy importante de experiencias exitosas en la región. En estos momentos estamos en un proceso de reestructura, refinanciamiento y relanzamiento, y más específicamente estamos pensando en crear una CVA (Comunidad Virtual de Aprendizaje) basado en el contenido actualizado de dicho metaspacio. Una parte de mis líneas de trabajo está en esta dirección, y estoy participando en un proyecto LACCIR dirigido por Regina Motz (del Instituto de Computación) en donde esta CVA de MISTICA es uno de los usuarios principales de dicho proyecto.

Tecnologías de la Información aplicadas a la Salud (2001)

Consultoría

VIOLA, A.

Asesor de la red Eurolatis para presentar proyectos en los programas marco de la Unión Europea

País: Cuba

Idioma: Español

Ciudad: La Habana

Disponibilidad: Restringida

Duración: 6 meses

Institución financiadora: Unión Europea

Palabras clave: TICs y desarrollo social Sociedad de la Información TICs y su uso en salud

Áreas de conocimiento:

Ingeniería y Tecnología / Ingeniería Eléctrica, Ingeniería Electrónica e Ingeniería de la Información /

Ingeniería de Sistemas y Comunicaciones / Tecnologías de la Comunicación en Información

Medio de divulgación: Internet

<http://www.eurolatis.upm.es>

Eurolatis era una red entre Europa y América Latina para el desarrollo de la Sociedad de la Información en nuestra región. La idea era organizar eventos coincidentes con los llamados en el programa marco de la Unión Europea a los efectos de presentar proyectos específicos en dichas convocatorias. Yo era miembro del Steering Committee por Uruguay. Es importante recalcar que en dicha época el tema de la sociedad de la información no estaba en la agenda de Uruguay, y que yo introduje en el tema en el país, vinculándome con el gobierno de turno. En este caso, participé en la evaluación, organización y seguimiento de proyectos presentados a la Unión Europea en temas relacionados con Tecnologías de la Información aplicadas a la Salud. El seguimiento consistió en asesorar a dos grupos para que presenten propuestas completas a los llamados de la Unión Europea.

Tecnologías de la Información aplicadas a la Educación (2000)

Consultoría

VIOLA, A.

Asesor de la red Eurolatis para presentar proyectos en los programas marco de la Unión Europea
País: Chile
Idioma: Español
Ciudad: Santiago de Chile - Montevideo
Disponibilidad: Restringida

Duración: 6 meses
Institución financiadora: Unión Europea
Palabras clave: TICs y desarrollo social TICs y su uso en educación Sociedad de la Información
Áreas de conocimiento:
Ingeniería y Tecnología / Ingeniería Eléctrica, Ingeniería Electrónica e Ingeniería de la Información / Ingeniería de Sistemas y Comunicaciones / Tecnologías de la Comunicación en Información
Medio de divulgación: Internet
<http://www.eurolatis.upm.es>
Eurolatis era una red entre Europa y América Latina para el desarrollo de la Sociedad de la Información en nuestra región. La idea era organizar eventos coincidentes con los llamados en el programa marco de la Unión Europea a los efectos de presentar proyectos específicos en dichas convocatorias. Yo era miembro del Steering Committee por Uruguay. Es importante recalcar que en dicha época el tema de la sociedad de la información no estaba en la agenda de Uruguay, y que yo introduje en el tema en el país, vinculándome con el gobierno de turno. En este caso, participé en la evaluación, organización y seguimiento de proyectos presentados a la Unión Europea en temas relacionados con Tecnologías de la Información aplicadas a la Educación. El seguimiento consistió en asesorar a dos grupos para que presenten propuestas completas a los llamados de la Unión Europea.

Miembro del Steering Committee de Eurolatis (1999)

Consultoría
VIOLA, A.
Eurolatis era una red Unión Europea - América Latina y Caribe, para el desarrollo de la Sociedad de la Información en la región
País: Uruguay
Idioma: Español
Disponibilidad: Restringida

Duración: 36 meses
Institución financiadora: Unión Europea
Palabras clave: TICs y desarrollo social Sociedad de la Información
Áreas de conocimiento:
Ingeniería y Tecnología / Ingeniería Eléctrica, Ingeniería Electrónica e Ingeniería de la Información / Ingeniería de Sistemas y Comunicaciones / Tecnologías de la Comunicación en Información
Eurolatis era una red entre Europa y América Latina y Caribe para el desarrollo de la Sociedad de la Información en nuestra región. La idea era organizar eventos coincidentes con los llamados en el programa marco de la Unión Europea a los efectos de presentar proyectos específicos en dichas convocatorias. Yo era miembro del Steering Committee por Uruguay. Es importante recalcar que en dicha época el tema de la sociedad de la información no estaba en la agenda de Uruguay, y que yo introduje en el tema en el país, vinculándome con el gobierno de turno.

Otras Producciones

CURSOS DE CORTA DURACIÓN DICTADOS

Análisis de algoritmos (2002)

VIOLA, A.
Perfeccionamiento
País: Argentina
Idioma: Español
Medio divulgación: Papel
Tipo de participación: Docente
Unidad: Escuela de Ciencias de la Computación (ECI)
Duración: 1 semana
Lugar: Universidad de Buenos Aires
Ciudad: Buenos Aires
Institución Promotora/Financiadora: Universidad de Buenos Aires
Palabras clave: Análisis de Algoritmos
Áreas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la

EDICIÓN O REVISIÓN

Proceedings LATIN 2014 (2014)

VIOLA, A. , PARDO, A.

Anales

País: Uruguay

Idioma: Inglés

Número de páginas: 700

Areas de conocimiento:

Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Teoría de la Computación

Selected papers from LATIN 2000 (2003)

VIOLA, A. , D. PANARIO , G. H. GONNET

Revista

País: Uruguay

Idioma: Inglés

Medio divulgación: Papel

Número de páginas: 350

Editorial: Elsevier

Amsterdam

Institución Promotora/Financiadora: Theoretical Computer Science (TCS)

Palabras clave: Teoría de la Computación

Areas de conocimiento:

Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Teoría de la Computación

Selected papers from CLEI 2002 (2003)

VIOLA, A.

Revista

País: Uruguay

Idioma: Inglés

Medio divulgación: Internet

Web: <http://www.clei.cl/cleiej/>

Número de páginas: 120

Editorial: CLEI

Chile

Institución Promotora/Financiadora: Centro Latinoamericano de Informática (CLEI)

Palabras clave: Informática

Areas de conocimiento:

Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Informática en general

Información adicional: Esta es una revista electrónica en donde se presentan versiones completas de los mejores trabajos aceptados en la Conferencia Latinoamericana de Informática en cada año. Yo fui presidente del Comité de Programa de CLEI 2002.

Proceedings of LATIN 2000 (Latin American Theoretical INformatics) (2000)

VIOLA, A. , D. PANARIO , G. H. GONNET

Anales

País: Uruguay

Idioma: Inglés

Medio divulgación: Papel

Número de páginas: 500

Editorial: Springer Verlag

Bonn

Institución Promotora/Financiadora: Lecture Notes in Computer Science - 1776

Palabras clave: Teoría de la Computación

Areas de conocimiento:

Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Teoría de la Computación

ORGANIZACIÓN DE EVENTOS

Conference on Space Efficient Data Structures, Streams and Algorithms (in honor of Ian Munro) (2013)

BRODNIK,A , LÓPEZ-ORTIZ, A. , RAMAN,V , VIOLA, A.

Congreso

Sub Tipo: Organización

Lugar: Canadá ,CANADÁ Waterloo, Ontario

Idioma: Inglés

Medio divulgación: Internet

Web: <http://www.fields.utoronto.ca/programs/scientific/13-14/efficient/>

Duración: 1 semanas

Palabras clave: Space Efficient Data Structures

Areas de conocimiento:

Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Teoría de la Computación

Formal Methods in Security (2007)

VIOLA, A. , G. BETARTE

Otro

Lugar: Uruguay ,Montevideo Montevideo

Idioma: Español

Medio divulgación: Internet

Duración: 1 semanas

Evento itinerante: SI

Institución Promotora/Financiadora: STIC-AMSUD

Palabras clave: Information Security

Areas de conocimiento:

Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Information Security

Información adicional: Tres días de seminario organizado en el marco de la red de cooperación con Francia STIC AMSUD

ITW Information Theory Workshop (2006)

VIOLA, A. , G. SEROUSSI

Concierto

Lugar: Uruguay ,Maldonado Punta del Este

Idioma: Inglés

Medio divulgación: CD-Rom

Web: <http://www.fing.edu.uy/itw06>

Duración: 1 semanas

Evento itinerante: SI

Catálogo: SI

Institución Promotora/Financiadora: Facultad de Ingeniería

Palabras clave: Teoría de la Información

Areas de conocimiento:

Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Teoría de la Información

Información adicional: Este es el evento más importante que se haya realizado en la región en Teoría de la Información y contó con la presencia de muchos de los líderes mundiales en sus respectivas áreas de investigación. Por otro lado, tuvo el agregado de que se organizó también la reunión del Board of Governors de la ITSOC (Sociedad Internacional de la Teoría de la Información. Por otro lado, y aprovechando dicho evento, se organizó un conjunto de charlas y actividades en la Facultad de Ingeniería con la participación de importantes investigadores dictando charlas estelares. Estas charlas estaban dirigidas a profesores y estudiantes, tanto de grado como de posgrado en Computación, Ingeniería Eléctrica y Matemáticas. Esta organización mereció la entrega de un diploma de reconocimiento oficial de parte de la IEEE en ISIT (la conferencia más prestigiosa en el mundo en el área) por la calidad mostrada en la organización del evento.

LATIN 2000 (2000)

VIOLA, A. , D. PANARIO

Congreso

Lugar: Uruguay ,Maldonado Punta del Este

Idioma: Inglés

Web: <http://www.fing.edu.uy/inco/eventos/latin-2000>

Duración: 1 semanas

Evento itinerante: SI

Catálogo: SI

Institución Promotora/Financiadora: Instituto de Computación

Palabras clave: Teoría de la Computación

Áreas de conocimiento:

Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Teoría de la Computación

Información adicional: LATIN es la conferencia más relevante a nivel mundial en Teoría de la Computación que se organiza en Latinoamérica y una de las más importantes del mundo en el área.

OTRA PRODUCCIÓN TÉCNICA

TUBA NUMBERS (2007)

VIOLA, A.

País: Estados Unidos

Idioma: Inglés

Medio divulgación: Internet

Web: <http://www.research.att.com/~njas/sequences/A124453>

secuencia A124453 en la The On-Line Encyclopedia of Integer Sequences de Neil Sloane

Palabras clave: linear probing hashing

Áreas de conocimiento:

Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / análisis de algoritmos

Información adicional: Esta secuencia ha sido la clave principal para resolver un problema de investigación abierto de nivel 48 (en un máximo de 50) aparecido en el volumen 3 de la colección The Art of Computer Programming del profesor Donald E. Knuth que es la colección más prestigiosa y la más vendida en la historia de la computación. De hecho este problema resuelto, generaliza el primer análisis hecho en la vida de D. Knuth en 1962, que generó su interés en crear esta colección de libros, y además se considera el inicio del área de análisis de algoritmos (una de mis principales ramas de investigación).

Bulletin of the European Association of Theoretical Computer Science (BEATCS) - News From Latin America (2001)

VIOLA, A.

País: Uruguay

Idioma: Inglés

Medio divulgación: Papel

Columna cuatrimestral sobre información de eventos en Teoría de la Computación realizados en la región

Lugar: Holanda, Amsterdam

Institución Promotora/Financiadora: European Association of Theoretical Computer Science

Palabras clave: Teoría de la Computación

Áreas de conocimiento:

Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Teoría de la Computación

Información adicional: Esta es una columna cuatrimestral que vengo llevando desde 2001 a la fecha, en donde informo sobre las actividades más relevantes en Teoría de la Computación realizadas en la región.

Evaluaciones

EVALUACIÓN DE PROYECTOS

EVALUACIÓN INDEPENDIENTE DE PROYECTOS

Presidente de concurso de tesis de Maestría CLEI - UNESCO (2009 / 2010)

Uruguay

Presidente de concurso de tesis de Maestría CLEI - UNESCO

Cantidad: Mas de 20

A partir de 2009, voy a ser presidente del concurso de tesis de Maestría CLEI - UNESCO.

Universidad de San Luis (2008 / 2008)

Argentina

Universidad de San Luis

Cantidad: Menos de 5
Evaluador externo de la propuesta de tesis de doctorado de Nora Reyes.

PDT - ANII (2006 / 2008)

Uruguay
PDT - ANII
Cantidad: Mas de 20
Perteneencia a Comisión Técnica Asesora en el área de Ciencias Básicas en llamados PDT y fondos Clemente Estable.

Conicet (2005 / 2008)

Argentina
Conicet
Cantidad: De 5 a 20
Evaluador periódico de varios proyectos de investigación financiados por dicha institución desde 2005.

cooperación internacional México - Argentina (2005 / 2008)

Argentina
cooperación internacional México - Argentina
Cantidad: Menos de 5
Evaluación de dos proyectos de cooperación internacional entre Argentina y México solicitado por la contraparte Argentina.

ECOS - cooperación Argentina - Francia (2004 / 2008)

Francia
ECOS - cooperación Argentina - Francia
Cantidad: Menos de 5
Evaluador de dos propuestas de proyectos ECOS entre grupos de investigación en Argentina y en Francia.

CLEI - UNESCO (1996 / 2008)

Uruguay
CLEI - UNESCO
Cantidad: Mas de 20
Desde 1996 he participado en varios tribunales del concurso Latinoamericano de Tesis de Maestría en Informática financiado conjuntamente por el CLEI (Centro Latinoamericano de Informática) y la UNESCO. He evaluado también varias tesis específicas en años en los que no he estado en el tribunal. A partir de 2009, voy a ser presidente de este tribunal. Estos premios se entregan anualmente con la Conferencia Latinoamericana de Informática.

EVALUACIÓN DE PUBLICACIONES

COMITÉ EDITORIAL

ACM Transactions on Algorithms (2009 / 2013)

Cantidad: Menos de 5

Combinatorics, Probability and Computing (2008 / 2013)

Cantidad: Menos de 5
Nueva revista online de Cambridge University Press

RAIRO (2005 / 2010)

Cantidad: Menos de 5
Revista francesa de informática teórica

IEEE Transactions on Information Theory (2002 / 2013)

Cantidad: Mas de 20
Es la revista más importante del mundo en Teoría de la Información

Random Structures and Algorithms (1998 / 2013)

Cantidad: Menos de 5
Es la revista más prestigiosa en Random Structures

Algorithmica (1998 / 2010)

Cantidad: Menos de 5
Una de las revistas más prestigiosas en algoritmos

Theoretical Computer Science (1996 / 2013)

Cantidad: De 5 a 20
Es una de las revistas más prestigiosas en Teoría de la Computación

EVALUACIÓN DE EVENTOS Y CONGRESOS

LATINCRYPT 2017 (2017)

Comité programa congreso
Cuba
Arbitrado

Universidad de la Habana
Conferencia de la cual fui co-fundador.

ANALCO 2018 (2017)

Comité programa congreso
Estados Unidos
Arbitrado

VIII Latin-American Algorithms, Graphs and Optimization Symposium (LAGOS 2015) (2014)

Brasil

Fourth International Conference of Emerging Applications of Information Technology (EAIT 2014) (2014)

India

Co-organizador de la escuela Combinatoria Analítica y Dinámica. Aplicaciones (2014)

Comité programa congreso
Argentina

UNGS
Escuela organizada en el marco del proyecto STIC-AMSUD "Dynalco". Con participación de estudiantes uruguayos.

ALEA 2015 (co-organizador) (2014)

Francia

ALEA es un evento anual realizado en Marsella creado por Philippe Flajolet. Es un ambiente de integración entre investigadores de matemáticas y de computación. Es un evento importante fundamentalmente para estudiantes. Yo he sido invitado a ser co-organizador del evento por Philippe Chassaing (Universidad de Nancy) quien es el presidente del comité de organización de ALEA 2015

LATINCRYPT 2014 (2014)

Brasil

Co-organizador de escuela de criptografía ASCrypto 2013 (2013)

Comité programa congreso
Brasil

Capes
<http://www.ic.unicamp.br/ascrypto2013/school.php> Co-organizador como miembro del Steering Committee de LATINCRYPT. Con participación de estudiantes de Uruguay.

LATIN 2014 (presidente del comité de programa) (2013)

Uruguay

Organizador del Workshop en Combinatoria Analítica (parte de CANADAM 2013) (2013)

Canadá

Conference on Space Efficient Data Structures, Streams and Algorithms (co-organizador de evento en homenaje a Ian Munro) (2013)

Canadá

La pagina Web del evento es <http://www.fields.utoronto.ca/programs/scientific/13-14/efficient/>

Third International Conference on Emergin Applications of Information Technology (EAIT 2012) (2012)

India

LATINCRYPT 2012 (2011)

Chile

Co-organizador de escuela de criptografía ASCrypto 2011 (2011)

Comité programa congreso
Brasil

FAPESP
<http://www.ic.unicamp.br/sp.ascrypto/> Evento realizado en el marco de LATINCRYPT, del cual soy miembro del Steering Committee. Con participación de estudiantes de Uruguay.

LATIN 2012 (2011)

Perú

LATIN es la Conferencia más prestigiosa en Teoría de la Computación organizada en la región y una de las más prestigiosas del mundo.

LATINCRYPT 2010 (2010)

México

Miembro del Steering Committee de LATINCRYPT que creó esta conferencia. Es la versión latinoamericana de la prestigiosa conferencia CRYPTO

Second International Conference on Emergin Applications of Information Technology (EAIT 2011) (2010)

India

Conference Proceedings publicados por la IEEE Computer Society Conference Publishing Services

LATIN 2010 (Latin American Theoretical INformatics) (2009)

México

Miembro del Comité de Programa

V Congreso Iberoamericano de Seguridad Informática (CIBSI09) (2009)

Uruguay

Miembro del Comité de Programa

Sistema nacional de investigador (2009)

Uruguay

Miembro de la Comisión Técnica de área de las Ingenierías y Tecnologías

ANALCO 2008 (Analytic Algorithms and Combinatorics) (2008)

Estados Unidos

Miembro de Comité de Programa Organizado por la SIAM

LATIN 2008 (Latin American Theoretical INformatics) (2008)

Brasil

Miembro de Comité de Programa Es la conferencia más relevante en la region en Teoría de la Computación y una de las más prestigiosas del mundo.

Sistema Nacional de Investigador (2008)

Uruguay

Miembro de la Comisión Técnica de área de las Ingenierías y Tecnologías

LAGOS/GRACO 2009 (2008)

Brasil

Miembro de Comité de Programa. Es una conferencia latinoamericana de gran relevancia internacional relacionado con Grafos, Algoritmos y Combinatoria. La Conferencia es en 2009.

CLEI 2007 (Conferencia Latinoamericana de Informática) (2007)

Costa Rica

Miembro de Comité de Programa

II Conference on Analysis of Algorithms (AofA7) (2007)

Francia

Miembro de Comité de Programa

IV Congreso Iberoamericano de Seguridad Informática (CIBSI07) (2007)

Argentina

Miembro de Comité de Programa

IFIP International Conference on Theoretical Computer Science (IFIP TCS 2006) (2006)

Chile

Miembro de Comité de Programa

LATIN 2006 (2006)

Chile

Miembro de Comité de Programa

IEEE Information Theory Workshop (ITW06) (2006)

Uruguay

Co-presidente junto con el Dr. Gadiel Seroussi (HP Labs, California). Es el evento más importante en Teoría de la Información organizado en la región, y contó con la presencia de los líderes mundiales en muchas de las áreas más relevantes en Teoría de la Información. Parte de la colaboración iniciada en el año 2000 con los Laboratorios HP, California en el tema de Teoría de la Información.

III Congreso Iberoamericano de Seguridad Informática (CIBSI 05) (2005)

Chile

Miembro de Comité de Programa

IFIP/ACM Latin American Networking Conference (LANC05) (2005)

Colombia

Miembro de Comité de Programa

Encuentro Internacional de Ciencias de la Computación (ENC 2005) (2005)

México

Miembro de Comité de Programa

I International Conference on the Analysis of Algorithms (AofA05) (2005)

España

Miembro del Comité de Programa. Fui uno de los miembros fundadores de la conferencia, y es la conferencia más importante en el mundo en el área.

Encuentro Internacional de Ciencias de la Computación (ENC 2004) (2004)

México

Miembro del Comité de Programa

CLEI 2003 (Conferencia Latinoamericana de Informatica) (2003)

Bolivia

Miembro del Comité de Programa

IFIP/ACM Latin American Networking Conference (LANC03) (2003)

Bolivia

Miembro del Comité de Programa

WAIT 2003 (Workshop Argentino de Informática Teórica) (2003)

Argentina

Miembro del Comité de Programa

CLEI 2002 (Conferencia Latinoamericana de Informatica) (2002)

Uruguay

Presidente del Comité de Programa

IFIP International Conference on Theoretical Computer Science (IFIP TCS 2002) (2002)

Canadá

Miembro del Comité de Programa

ACM - SIGCOMM Conferencia sobre Comunicación de Datos en Latinoamérica y el Caribe (2001)

Costa Rica

Miembro de Comité de Programa Fui uno de los miembros fundadores de esta conferencia, que luego derivó en IFIP/ACM Latin American Networking Conference.

LATIN 2000 (Latin American Theoretical INformatics) (2000)

Uruguay

Organizador del evento junto con el Dr. Daniel Panario (Universidad de Carleton, Canadá). Es una de las conferencias más importantes del mundo en Teoría de la Computación y contó con la presencia de muchos de los líderes mundiales en áreas fundamentales.

WAIT 1997 (Workshop Argentino de Informática Teórica) (1997)

Argentina

Miembro del Comité de Programa

EVALUACIÓN DE PREMIOS

Premios Anuales de Literatura (2010 / 2010)

Uruguay

Cantidad: Menos de 5

Ministerio de Educación y Cultura

categoría: OBRAS SOBRE INVESTIGACIÓN Y DIFUSIÓN CIENTÍFICA.

EVALUACIÓN DE CONVOCATORIAS CONCURSABLES

ANII - diferentes convocatorias (2010 / 2013)

Uruguay

Cantidad: Mas de 20

ANII

Varias evaluaciones realizadas para diversos programas de ANII ya sea como miembro de comite de programa o como evaluador.

Acreditación de Carreras Universitarias de Computación en Argentina (2010 / 2011)

Argentina

Cantidad: De 5 a 20

CONEAU

Evaluador extranjero en el proceso de acreditación de carreras de Computación en Argentina.

Proyectos de Iniciación a la Investigación Científica (2009)

Uruguay

Cantidad: De 5 a 20

CSIC - UDELAR

Participación en la comisión de evaluación

FCE (2008)

Uruguay
Cantidad: De 5 a 20
ANII
Integrante de la comisión técnica del área básica

PDT (2006)

Uruguay
Cantidad: De 5 a 20
Ministerio de Educación y Cultura
Integrante de comisión Técnica del área básica

JURADO DE TESIS

Doctorado en Computación (2016)

Jurado de mesa de evaluación de tesis
Sector Extranjero/Internacional/Enseñanza superior / Universite de Paris XIII (Paris-Nord) , Francia
Tesis de doctorado de Nicolás Rollin.

Doctorado en Computación (2015 / 2016)

Jurado de mesa de evaluación de tesis
Sector Extranjero/Internacional/Enseñanza superior / Universite de Paris XIII (Paris-Nord) , Francia
Miembro externo de tribunal de doctorado del estudiante Nicolas Rolin.

Formación de RRHH

TUTORÍAS CONCLUIDAS

POSGRADO

Combinatoria Analítica y Aplicaciones (2014)

Tesis de maestría
Sector Educación Superior/Público / Programa de Desarrollo de las Ciencias Básicas / Programa de Desarrollo de las Ciencias Básicas , Uruguay
Programa: Maestría en Informática
Tipo de orientación: Tutor único o principal
Nombre del orientado: Pablo Rotondo
País/Idioma: Uruguay, Español
Palabras Clave: Combinatoria Analítica
Areas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / combinatoria analítica

Tree models: Algorithms and Information Theoretic Properties (2009)

Tesis de doctorado
Sector Educación Superior/Público / Universidad de la República / Facultad de Ingeniería - UDeLaR , Uruguay
Programa: Doctorado en Informática (UDELAR-PEDECIBA)
Nombre del orientado: Alvaro Martin
País/Idioma: Uruguay, Inglés
Palabras Clave: Type classes Tree Models
Areas de conocimiento:
Ingeniería y Tecnología / Ingeniería Eléctrica, Ingeniería Electrónica e Ingeniería de la Información / Telecomunicaciones / Teoría de la Información
El orientador de Tesis fue el Dr. Gadiel Seroussi.

Análisis del algoritmo de compresión PPM (2006)

Tesis de maestría
Sector Educación Superior/Público / Universidad de la República / Facultad de Ingeniería - UDeLaR , Uruguay
Programa: Maestría en Informática (UDELAR-PEDECIBA)

Nombre del orientado: Jorge Merlino
Medio de divulgación: Papel
País/Idioma: Uruguay, Español
Palabras Clave: Algoritmo PPM
Áreas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Teoría de la Información
Supervisor de estudios y co-orientador de tesis junto con Marcelo Weinberger (HP Labs, California)

Implementación eficiente de modelos de Markov dispersos usando algoritmos genéticos (2005)

Tesis de maestría
Sector Educación Superior/Público / Universidad de la República / Facultad de Ingeniería - UDeLaR, Uruguay
Programa: Maestría en Informática (UDELAR-PEDECIBA)
Nombre del orientado: Alix Lhéritier
Medio de divulgación: Papel
País/Idioma: Uruguay, Español
Palabras Clave: Modelos de Markov dispersos
Áreas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Teoría de la Información
Supervisor de estudios y co-orientador de tesis junto con Gadiel Seroussi (HP Labs, California)

Texture Mixing via Universal Simulation (2005)

Tesis de maestría
Sector Educación Superior/Público / Universidad de la República / Facultad de Ingeniería - UDeLaR, Uruguay
Programa: Maestría en Informática (UDELAR-PEDECIBA)
Nombre del orientado: Gustavo Brown
Medio de divulgación: Papel
País/Idioma: Uruguay, Inglés
Palabras Clave: simulación de texturas Algoritmo de Lempel-Ziv
Áreas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Teoría de la Información
Orientación de Tesis de parte de Gadiel Seroussi (HP Labs, California) y Guillermo Sapiro (U. de Minnesota)

GRADO

Funciones Booleanas inmunes a la correlación y ataques a AES en tarjetas inteligentes (2017)

Tesis/Monografía de grado
Sector Educación Superior/Público / Universidad de la República / Facultad de Ingeniería - UDeLaR, Uruguay
Programa: Licenciatura en Computación
Tipo de orientación: Tutor único o principal
Nombre del orientado: Francisco Castro
País/Idioma: Uruguay, Español
Palabras Clave: ataque AES
Áreas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Funciones Booleanas
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / criptografía

Generación Aleatoria de Funciones Booleanas inmunes a la correlación de menor peso (2015)

Tesis/Monografía de grado
Sector Educación Superior/Público / Universidad de la República / Facultad de Ingeniería - UDeLaR, Uruguay
Programa: Ingeniería en Computación
Tipo de orientación: Tutor único o principal
Nombre del orientado: Sebastián Fonseca / María Cecilia García
País/Idioma: Uruguay, Español
Áreas de conocimiento:

Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / criptografía

Prueba formal de algoritmos de firma digital y sus implementaciones usando asistentes de prueba (2014)

Tesis/Monografía de grado
Sector Educación Superior/Público / Universidad de la República / Facultad de Ingeniería - UDeLaR,
Uruguay
Programa: Ingeniería en Computación
Nombre del orientado: Adrian Silveira
País/Idioma: Uruguay, Español
Palabras Clave: Firma Digital Asistente de Pruebas Métodos Formales
Areas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / criptografía
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Métodos Formales
Co-dirección con Gustavo Betarte en colaboración con Gilles Barthes (España).

Implementación eificientes de algoritmos de decodificación por listas de los códigos Reed-Solomon (2009)

Tesis/Monografía de grado
Sector Educación Superior/Público / Universidad de la República / Facultad de Ingeniería - UDeLaR,
Uruguay
Programa: Ingeniería en Computación
Nombre del orientado: Cecilia Parodi y Gaston Simone
Medio de divulgación: Papel
País/Idioma: Uruguay, Español
Palabras Clave: Decodificación por Listas Códigos Reed - Solomon
Areas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Teoría de Códigos
Proyecto co-tutoreado por Fernando fernández y con la participación y proyesta de proyecto de Gadiel Seroussi (HP Labs, California)

Generación aleatoria eficiente de funciones booleanas resilientes (2009)

Tesis/Monografía de grado
Sector Educación Superior/Público / Universidad de la República / Facultad de Ingeniería - UDeLaR,
Uruguay
Programa: Ingeniería en Computación
Nombre del orientado: Nicolàs Carrasco
País/Idioma: Uruguay, Español
Palabras Clave: funciones booleanas resilientes
Areas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Funciones booleanas, criptografía
En colaboración con Jean-Marie Le Bars de la Universidad de Caen.

Predicción de Estructura Secundaria de Proteínas (2006)

Tesis/Monografía de grado
Sector Educación Superior/Público / Universidad de la República / Facultad de Ingeniería - UDeLaR,
Uruguay
Programa: Ingeniería en Computación
Nombre del orientado: Elisa Budelli
Medio de divulgación: Papel
País/Idioma: Uruguay, Español
Palabras Clave: predicción de estructura secundaria de proteínas
Areas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / bioinformática
Trabajo co-dirigido con Fernando Alvarez de la Facultad de Ciencias

Algoritmos óptimos de compresión (2004)

Tesis/Monografía de grado
Sector Educación Superior/Público / Universidad de la República / Facultad de Ingeniería - UDeLaR,
Uruguay

Programa: Ingeniería en Computación
Nombre del orientado: Florencia da Silveira: Karina Alvarez
País/Idioma: Uruguay, Español
Palabras Clave: Algoritmo Context
Areas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Teoría de la Información
Co-dirigido con Alvaro Martín

Corrección de errores para distribución de datos en redes (2004)

Tesis/Monografía de grado
Sector Educación Superior/Público / Universidad de la República / Facultad de Ingeniería - UDeLaR , Uruguay
Programa: Ingeniería en Computación
Nombre del orientado: Fernando Fernández
Medio de divulgación: Papel
País/Idioma: Uruguay, Español
Palabras Clave: Codigos correctores de errores
Areas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Teoría de Códigos
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Comunicaciones

Codigos de paridad de baja densidad (2003)

Tesis/Monografía de grado
Sector Educación Superior/Público / Universidad de la República / Facultad de Ingeniería - UDeLaR , Uruguay
Programa: Ingeniería en Computación
Nombre del orientado: Alix Lhéritier
Medio de divulgación: Papel
País/Idioma: Uruguay, Español
Palabras Clave: Codigos LDPC
Areas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Teoría de Códigos

El comercio electrónico y los sistemas de pago online (2003)

Tesis/Monografía de grado
Sector Educación Superior/Público / Universidad de la República / Facultad de Ingeniería - UDeLaR , Uruguay
Programa: Ingeniería en Computación
Nombre del orientado: César Ponce: José Pedro Rabinovich
Medio de divulgación: Papel
País/Idioma: Uruguay, Español
Palabras Clave: pagos online
Areas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / criptografía

Simulación de un mercado de transacciones financieras por internet (2002)

Tesis/Monografía de grado
Sector Educación Superior/Público / Universidad de la República / Facultad de Ingeniería - UDeLaR , Uruguay
Programa: Ingeniería en Computación
Nombre del orientado: Luján Camino; Marcos Viera; Diego Borghi; Elisa Bittencourt
Medio de divulgación: Papel
País/Idioma: Uruguay, Español
Palabras Clave: pagos online
Areas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / criptografía

Inserción de marcas de tiempo en certificados digitales (2002)

Tesis/Monografía de grado
Sector Educación Superior/Público / Universidad de la República / Facultad de Ingeniería - UDeLaR
, Uruguay
Programa: Ingeniería en Computación
Nombre del orientado: Ricardo Martínez
Medio de divulgación: Papel
País/Idioma: Uruguay, Español
Palabras Clave: marcas de tiempo
Areas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la
Computación / criptografía
En coordinación con la autoridad certificadora del correo uruguayo.

Criptografía para dispositivos de bajos recursos (2001)

Tesis/Monografía de grado
Sector Educación Superior/Público / Universidad de la República / Facultad de Ingeniería - UDeLaR
, Uruguay
Programa: Ingeniería en Computación
Nombre del orientado: Santiago Jaureche; Jorge Merlino
Medio de divulgación: Papel
País/Idioma: Uruguay, Español
Palabras Clave: dispositivos de bajos recursos
Areas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la
Computación / criptografía

Estudio de Transacciones electrónicas en internet (2001)

Tesis/Monografía de grado
Sector Educación Superior/Público / Universidad de la República / Facultad de Ingeniería - UDeLaR
, Uruguay
Programa: Ingeniería en Computación
Nombre del orientado: Daniel Brignardello
Medio de divulgación: Papel
País/Idioma: Uruguay, Español
Palabras Clave: transacciones electrónicas por internet
Areas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la
Computación / criptografía

Relevamiento de escenarios y técnicas para realización de proyectos de comercio electrónico (2000)

Tesis/Monografía de grado
Sector Educación Superior/Público / Universidad de la República / Facultad de Ingeniería - UDeLaR
, Uruguay
Programa: Ingeniería en Computación
Nombre del orientado: Leonardo Domínguez; Cecilia Fernández
Medio de divulgación: Papel
País/Idioma: Uruguay, Español
Palabras Clave: comercio electrónico
Areas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la
Computación / criptografía

Sistema de comercio electrónico (1999)

Tesis/Monografía de grado
Sector Educación Superior/Público / Universidad de la República / Facultad de Ingeniería - UDeLaR
, Uruguay
Programa: Ingeniería en Computación
Nombre del orientado: Pablo Torres
País/Idioma: Uruguay, Español
Palabras Clave: comercio electrónico
Areas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la
Computación / criptografía

Inserción de marcas de agua en imágenes digitales (1999)

Tesis/Monografía de grado
Sector Educación Superior/Público / Universidad de la República / Facultad de Ingeniería - UDeLaR
, Uruguay
Programa: Ingeniería en Computación
Nombre del orientado: Fabian Martínez; Gabriela Delfino
País/Idioma: Uruguay, Español
Palabras Clave: watermarking
Áreas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la
Computación / criptografía

Implementación de un buscador en internet de información universitaria, académica y científica en el dominio .uy (1999)

Tesis/Monografía de grado
Sector Educación Superior/Público / Universidad de la República / Facultad de Ingeniería - UDeLaR
, Uruguay
Programa: Ingeniería en Computación
Nombre del orientado: J. P. Fernández; Uruguay Larre Borges; Francisco Pereira
Medio de divulgación: Papel
País/Idioma: Uruguay, Español
Palabras Clave: recuperación de información
Áreas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la
Computación / Sistemas de Información

Construcción de un prototipo para la búsqueda de información académica en Uruguay (1998)

Tesis/Monografía de grado
Sector Educación Superior/Público / Universidad de la República / Facultad de Ingeniería - UDeLaR
, Uruguay
Programa: Ingeniería en Computación
Nombre del orientado: Federico Molfino; P.ablo Sartor; Fernando Vignali
País/Idioma: Uruguay, Español
Palabras Clave: recuperación de información
Áreas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la
Computación / Sistemas de Información

Buscador Académico Uruguayo (1997)

Tesis/Monografía de grado
Sector Educación Superior/Público / Universidad de la República / Facultad de Ingeniería - UDeLaR
, Uruguay
Programa: Ingeniería en Computación
Nombre del orientado: Alfredo Espasandín; Ricardo Martínez
Medio de divulgación: Papel
País/Idioma: Uruguay, Español
Palabras Clave: recuperación de información
Áreas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la
Computación / Sistemas de Información

TUTORÍAS EN MARCHA

POSGRADO

Análisis Dinámico en Combinatoria de Palabras (2015)

Tesis de doctorado
Sector Educación Superior/Público / Facultad de Ingeniería - UDeLaR , Francia
Programa: Doctorado en Informática (UDELAR-PEDECIBA)
Tipo de orientación: Cotutor en pie de igualdad
Nombre del orientado: Pablo Rotondo
País/Idioma: Francia, Inglés
Palabras Clave: Análisis dinámico de algoritmos
Áreas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la
Computación

Doctorado en cotutela con la Universidad de Paris 7. La orientadora del lado francés es Valérie Berthé, contando con la activa participación de Brigitte Vallée de la Universidad de Caen.

Seguridad en redes GSM (2011)

Tesis de maestría
Sector Educación Superior/Público / Universidad de la República / Facultad de Ingeniería - UDeLaR,
Uruguay
Programa: Maestría en Ingeniería (Ingeniería Eléctrica)
Nombre del orientado: Eduardo Cota
País/Idioma: Uruguay, Español
Palabras Clave: Redes GSM Seguridad
Áreas de conocimiento:
Ingeniería y Tecnología / Ingeniería Eléctrica, Ingeniería Electrónica e Ingeniería de la Información /
Telecomunicaciones / Seguridad en Redes GSM
Co-dirección de tesis junto con Eduardo Giménez. El supervisor de estudios es Pablo Belzarena.

OTRAS

Criptografía post-cuántica basada en latices (2018)

Otras tutorías/orientaciones
Sector Educación Superior/Público / Universidad de la República / Facultad de Ingeniería , Uruguay
Tipo de orientación: Tutor único o principal
Nombre del orientado: Bruno Scarone
País/Idioma: Uruguay, Español
Palabras Clave: criptografía latices algoritmos
Áreas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la
Computación / criptografía, combinatoria
Proyecto de grado en Ingeniería en computación

Relevamiento de técnicas de clusterización de identidades en criptomonedas (2018)

Otras tutorías/orientaciones
Sector Educación Superior/Público / Universidad de la República / Facultad de Ingeniería , Uruguay
Tipo de orientación: Cotutor en pie de igualdad
Nombre del orientado: Alex Rostan, Fabricio Garin, Lucas Bouissa
País/Idioma: Uruguay, Español
Palabras Clave: blockchain monedas digitales
Áreas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la
Computación e Información / criptografía
Proyecto de grado en co-dirección con Germán Ferrari

Relevamiento de ataques de seguridad a las redes de Bitcoin y Ethereum (2018)

Otras tutorías/orientaciones
Sector Educación Superior/Público / Universidad de la República / Facultad de Ingeniería , Uruguay
Tipo de orientación: Cotutor en pie de igualdad
Nombre del orientado: Jonathan Javiel, Mauro Saravia, Federico Paredes
País/Idioma: Uruguay, Español
Palabras Clave: blockchain seguridad de la información
Áreas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la
Computación e Información / criptografía, seguridad de la información
Proyecto de grado de Ingeniería en Computación en codirección con Germán Ferrari

Análisis de monedas digitales (2018)

Otras tutorías/orientaciones
Sector Educación Superior/Público / Universidad de la República / Facultad de Ingeniería , Uruguay
Tipo de orientación: Tutor único o principal
Nombre del orientado: Gabriel Yermán
País/Idioma: Uruguay, Español
Palabras Clave: monedas digitales
Áreas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la
Computación e Información / criptografía, seguridad de la información

Criptoanálisis de texto enviado por tupamaros en el exterior a la cárcel de Libertad (2018)

Otras tutorías/orientaciones
Sector Educación Superior/Público / Programa de Desarrollo de las Ciencias Básicas / Área Informática (PEDECIBA) , Uruguay
Tipo de orientación: Cotutor en pie de igualdad
Nombre del orientado: Francisco Castro
País/Idioma: Uruguay, Español
Palabras Clave: criptografía seguridad de la información
Áreas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación e Información / criptografía, seguridad de la información
Tesis de Maestría del Pedeciba Informática en codirección con Joachim von zur Gathen (Universidad de Bonn, Alemania)

Funciones Booleanas inmunes a la correlación. (2017)

Otras tutorías/orientaciones
Sector Educación Superior/Público / Universidad de la República / Facultad de Ingeniería , Uruguay
Tipo de orientación: Tutor único o principal
Nombre del orientado: Octavio Pérez Kepner
País/Idioma: Uruguay, Español
Palabras Clave: funciones booleanas inmunidad a la correlación
Áreas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / combinatoria, criptografía
Proyecto de grado de Ingeniería en Computación

Otros datos relevantes

PREMIOS, HONORES Y TÍTULOS

Invitado a ser keynote speaker en AofA 2013. (2012)

(Internacional)
Steering Committee de Analysis of Algorithms
Este es el evento anual más importante de la comunidad científica de Combinatoria Analítica. En esta charla presentaré la historia del problema Linear Probing Hashing, en homenaje a los 50 años de su primer análisis. Este primer análisis realizado en 1963 por D. E. Knuth es considerado el origen del área de Análisis de Algoritmos. Por otro lado, es considerado también como el problema que motivó a D. E. Knuth a publicar la colección de libros más leída vendida en la historia de la Computación: The Art of Computer Programming. Mis trabajos científicos relacionados con varios análisis de este problema, aparecen citados en el volumen 3 de dicha colección. El análisis de varias de las variables aleatorias relacionadas con este problema, muestran la riquísima estructura del mismo, y su inesperada relación con otros problemas fundamentales de la Combinatoria. En dicha charla, además de presentar los resultados científicos mostraré también su importancia histórica en el desarrollo de nuestra comunidad académica e hitos muy reconocidos por su impacto posterior.

Sistema Nacional de Investigador (Nivel II) (2009)

ANII

Citado en Analytic Combinatorics Philippe Flajolet and Robert Sedgewick. Este es el libro fundamental en una de mis principales áreas de investigación como lo es el de la combinatoria analítica y su uso en el análisis de algoritmos. (2009)

<http://algo.inria.fr/flajolet/Publications/books.html>

Autor de la secuencia TUBA NUMBERS (2007)

(Internacional)
<http://www.research.att.com/~njas/sequences/A124453>
Autor de la secuencia A124453 en la Online Encyclopedia of Integer Sequences de Neil Sloane llamada Tuba Numbers (<http://www.research.att.com/~njas/sequences/A124453>). Esta secuencia ha sido la clave principal para resolver un problema de investigación abierto de dificultad 48 (sobre

un maximo de 50) aparecido en el volumen 3 de la coleccion The Art of Computer Programming del profesor Donald E. Knuth, que es la coleccion de libros mas prestigiosa y mas vendida de la historia de la computacion. Este problema generaliza el primer analisis realizado por D. Knuth en 1962, que dio origen a esta coleccion de libros y es considerado ademas el inicio del area de Analisis de Algoritmos (una de mis areas de investigacion)

Fondo Nacional de Investigador (Nivel II) -con financiamiento (2005)

DICyT

Trabajos citados en Handbook of Data Structures and Applications Dinesh P. Mhta y Sartaj Sahni Capman & Hall/CRC (2004) ISBN-13: 978-1584884354. Enciclopedia de referencia en Estructuras de Datos y Algoritmos. (2004)

Capman & Hall/CRC

Citado en Modern Computer Algebra Joachim von zur Gathen and Jürgen Gerhard Cambridge University Press (2003) ISBN:0521826462. Este es el libro de más relevancia mundial en el tema. (2003)

<http://math-www.uni-paderborn.de/mca/>

Citado en articulo History of the Analysis of Algorithms (AofA): Part I: 1993 - 1998 (Dagstuhl Period), BEATCS, 77, 43-62, June 2002. (2002)

Dagstuhl Seminars

Citado en Average Case Analysis of Algorithms on Sequences de W. Szpankowski, Wiley-Interscience in Discrete Matematics and Optimization (2001) ISBN: 0-471-24063-X. (2001)

Wiley-Interscience

Keynote Speaker: 'Analysis of Rabin's Irreducibility Test for Polynomials over Finite Fields' en 7th Seminar on Analysis of Algorithms, evento mundial más importante del área. (2001)

AofA

Fondo Nacional de Investigador (Nivel II) - sin financiamiento (2000)

DICyT

Trabajos citados en Algorithms and Theory of Computation Handbook Mikhail J. Atallah CRC-PRESS (1998) ISBN-13: 978-0849326493. Enciclopedia en Algoritmos y Teoría de la Computación (1998)

CRC-PRESS

Citado en The Art of Computer Programming: Volume 3: "Sorting and Searching" Second Edition (1998) de Donald E. Knuth, Adisson-Wesley SBN: 0-201-89685-0. Es la colección de libros más prestigiosa y más vendida en la historia de la computación. (1997)

<http://www-cs-faculty.Stanford.EDU/~knuth/>

International Student Fee Waiver (1990)

Universidad de Waterloo

Student Fellowship (1989)

NSERC - Canadá

BECA PEDECIBA para realizar posgrado en Canadá (1987)

Pedeciba

PRESENTACIONES EN EVENTOS

Philippe Flajolet and Analytic Combinatorics (2011)

Simposio

Philippe Flajolet and his theoretical contributions in the analysis of hashing algorithms

Francia

Tipo de participación: Conferencista invitado

Nombre de la institución promotora: INRIA

Palabras Clave: Hashing Algorithms

Areas de conocimiento:

Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / combinatoria analítica

Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / analisis de algoritmos

Es un evento especial organizado en honor a Philippe Flajolet,, líder de nuestra área de investigación, miembro de la Academia de Ciencias de Francia y quien falleció en marzo 2011.

Escuela de Criptografía SP-ASCrypto (2011)

Simposio

Boolean Functions in cryptography

Brasil

Tipo de participación: Conferencista invitado

Nombre de la institución promotora: CNPQ

Palabras Clave: funciones booleanas

Areas de conocimiento:

Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / criptografía

Es una escuela de criptografía que estamos organizando en el marco de LATINCrypt. La idea es organizar una conferencia en los años pares, y una escuela en los años impares. LATINCrypt fue creada en 2010 en el marco del proyecto STIC-AMSUD FMCRYPTO, y es la versión regional de la prestigiosa conferencia Crypto. El objetivo es fomentar el desarrollo de grupos de investigación en Criptografía en la región y la formación de recursos humanos radicados en nuestros países.

Invitacion a participar en el seminario del laboratorio (2010)

Seminario

Distributional analysis of the parking problem and the Robin Hood Linear probing algorithm with buckets

Francia

Tipo de participación: Expositor oral

Nombre de la institución promotora: Ecole Polytechnique

Palabras Clave: hashing parking problem with buckets linear probing with buckets Tuba Numbers

Areas de conocimiento:

Ciencias Naturales y Exactas / Matemáticas / Matemática Aplicada / Analisis de algoritmos y combinatoria

Invitacion a realizar trabajos de investigacion conjunta y presentacion de mis resultados recientes de investigacion.

(2009)

Simposio

Some asymptotic issues related with the exact distribution of Individual Displacements in Linear Probing Hashing

Canadá

Tipo de participación:

Palabras Clave: linear probing hashing

Areas de conocimiento:

Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / analisis de algoritmos

Dagstuhl Seminar on Data Structures (2008)

Seminario

Efficient Data Structures for Universal Denoising

Alemania

Tipo de participación: Expositor oral

Carga horaria: 30

Nombre de la institución promotora: Schloss Dagstuhl - Leibniz Center for Informatics

Los seminarios Dagstuhl, son eventos en los que se participa sólo por invitación. Un grupo de líderes mundiales en un área temática organiza uno de estos seminarios y realiza invitación a expertos y estudiantes de doctorado en dichas áreas para realizar presentaciones y realizar trabajos de investigación conjunta. Sacado de su pagina Web: Schloss Dagstuhl - Leibniz Center for Informatics is the world's premier venue for informatics. It enables the international elite, promising young researchers and practitioners alike to gather together to discuss their views and research findings. The Center promotes fundamental and applied research, continuing and advanced academic education, and the transfer of knowledge between those involved in the research side and application side of informatics. The key instrument for promoting research are the Dagstuhl Seminars, which bring together internationally renowned leading scientists for the purpose of exploring a cutting-edge informatics topic. The friendly and open climate at the conference center promotes a culture of communication and exchange among the seminar participants. The non-profit Center is a member of the Leibniz Association and is funded jointly by the German federal government and a number of state governments.

Grand Challenges in Computer Science Research in Latin America Workshop (2008)

Encuentro

INFORMATION TECHNOLOGIES TO THE HELP OF CITIZEN PARTICIPATION IN PUBLIC DECISIONS AND PUBLIC EDUCATION

Argentina

Tipo de participación: Expositor oral

Nombre de la institución promotora: CLEI y SBC (Sociedad Brasileira de Computación)

Palabras Clave: participación ciudadana tecnologías de la información y educación decisiones públicas

Areas de conocimiento:

Ingeniería y Tecnología / Ingeniería Eléctrica, Ingeniería Electrónica e Ingeniería de la Información / Ingeniería de Sistemas y Comunicaciones / Sociedad de la Información y Conocimiento

En este evento, que contó también con la participación de Microsoft (auspiciante de la iniciativa LACCIR) se discutieron sobre diversas iniciativas orientadas a pensar grandes áreas temáticas de investigación y desarrollo vinculadas a la computación y sus usos sociales, a los efectos de generar un movimiento regional de apoyo al financiamiento de dichas actividades de alto impacto en el desarrollo de la región. Mi actividad consistió en presentar la exposición que comento, participar en los grupos de trabajos formados en dicho evento, y participar en la elaboración de un documento final.

Workshop on Information Theory and Applications (2007)

Simposio

Combinatorial characterization of Resilient Functions

Estados Unidos

Tipo de participación: Expositor oral

Nombre de la institución promotora: Universidad de San Diego

Es un evento por invitación y es uno de los eventos más importantes y relevantes en Teoría de la Información.

11th seminar on Analysis of Algorithms (2006)

Seminario

Optimal prefix codes for pairs of geometrically-distributed random variables

Bélgica

Tipo de participación: Expositor oral

Nombre de la institución promotora: Alden Biesen

Este es un evento por invitación organizado por la comunidad internacional de Analisis de Algoritmos (a la cual pertenezco activamente) y es la continuación de los seminarios Dagstuhl en el área.

10th Seminar on Analysis of Algorithms (2004)

Seminario

Adaptive Sampling Strategies for Quickselect

Estados Unidos

Tipo de participación: Expositor oral

Nombre de la institución promotora: MSRI

Este es un evento por invitación organizado por la comunidad internacional de Analisis de

Algoritmos (a la cual pertenezco activamente) y es la continuación de los seminarios Dagstuhl en el área.

9th Seminar on Analysis of Algorithms (2003)

Seminario

On worst case Robin Hood Hashing

Italia

Tipo de participación: Expositor oral

Nombre de la institución promotora: Universidad de Florencia

Este es un evento por invitación organizado por la comunidad internacional de Analisis de Algoritmos (a la cual pertenezco activamente) y es la continuación de los seminarios Dagstuhl en el área.

Workshop on Combinatorics, Algorithms and Applications (2003)

Simposio

Adaptive Sampling Strategies for Quickselect

Brasil

Tipo de participación: Conferencista invitado

Nombre de la institución promotora: Universidad de San Pablo

8th Seminar on Analysis of Algorithms (2002)

Seminario

Exact distribution of individual displacements in linear probing hashing

Austria

Tipo de participación: Expositor oral

Nombre de la institución promotora: Universidad de Viena

Este es un evento por invitación organizado por la comunidad internacional de Analisis de Algoritmos (a la cual pertenezco activamente) y es la continuación de los seminarios Dagstuhl en el área.

KnuthFest (2002)

Encuentro

KnuthFest

Estados Unidos

Tipo de participación: Otros

Nombre de la institución promotora: Universidad de Stanford

KnuthFest fue un evento de celebración de los 64 años de D. E. Knuth. El Dr. Knuth es la persona más relevante de la segunda mitad del siglo XX en Computación. Es el autor de la famosa colección de libros "The Art of Computer Programming", que es la colección de libros más vendida y de mayor impacto en la historia de la computación. Por otro lado es el creador del área de Análisis de Algoritmos, una de mis principales áreas de investigación. Este fue un evento realizado por invitación, en donde sólo participaron 70 personas. No hice una presentación en este evento, pero en la charla del Dr. Svante Janson nombraron mis trabajos relacionados con "Linear Probing Hashing" que aparecen referenciados en el volumen 3 de "The Art of Computer Programming".

7th Seminar on Analysis of Algorithms (2001)

Seminario

Analysis of Rabin's Irreducibility Test for Polynomials over Finite Fields

Francia

Tipo de participación: Conferencista invitado

Nombre de la institución promotora: Universidad de Caen

Este es un evento por invitación organizado por la comunidad internacional de Analisis de Algoritmos (a la cual pertenezco activamente) y es la continuación de los seminarios Dagstuhl en el área. En esta ocasión fui invitado a dar una charla estelar de 1 hora de duración.

Montreal - Ottawa Analysis of Algorithms Workshop (2001)

Simposio

The Effect of Deletions on Different Insertion Disciplines for Hash Tables

Canadá

Tipo de participación: Conferencista invitado

Nombre de la institución promotora: Universidad de Carleton

6th Seminar on Analysis of Algorithms (2000)

Seminario

Open problems related with Linear Probing Hashing with Buckets

Polonia

Tipo de participación: Expositor oral

Nombre de la institución promotora: Universidad de Gdansk

Este es un evento por invitación organizado por la comunidad internacional de Analisis de Algoritmos (a la cual pertenezco activamente) y es la continuación de los seminarios Dagstuhl en el área.

Encuentro Brasileiro de Combinatoria (2000)

Encuentro

The symbolic method in combinatorics

Brasil

Tipo de participación: Conferencista invitado

Nombre de la institución promotora: Universidad de San Pablo

5th Seminar on Analysis of Algorithms (1999)

Seminario

The Effect of Deletions on Different Insertion Disciplines for Hash Tables

España

Tipo de participación: Expositor oral

Nombre de la institución promotora: Universidad Politécnica de Catalunya

Este es un evento por invitación organizado por la comunidad internacional de Analisis de Algoritmos (a la cual pertenezco activamente) y es la continuación de los seminarios Dagstuhl en el área.

Dagstuhl Seminar on Data Structures (1997)

Seminario

Analysis of the total displacement in a linear probing hash table.

Alemania

Tipo de participación: Expositor oral

Nombre de la institución promotora: Schloss Dagstuhl - Leibniz Center for Informatics

Los seminarios Dagstuhl, son eventos en los que se participa sólo por invitación. Un grupo de líderes mundiales en un área temática organiza uno de estos seminarios y realiza invitación a expertos y estudiantes de doctorado en dichas áreas para realizar presentaciones y realizar trabajos de investigación conjunta. Sacado de su pagina Web: Schloss Dagstuhl - Leibniz Center for Informatics (German: Schloss Dagstuhl - Leibniz-Zentrum für Informatik GmbH) is the world's premier venue for informatics. It enables the international elite, promising young researchers and practicians alike to gather together to discuss their views and research findings. The Center promotes fundamental and applied research, continuing and advanced academic education, and the transfer of knowledge between those involved in the research side and application side of informatics. The key instrument for promoting research are the Dagstuhl Seminars, which bring together internationally renowned leading scientists for the purpose of exploring a cutting-edge informatics topic. The friendly and open climate at the conference center promotes a culture of communication and exchange among the seminar participants. The non-profit Center is a member of the Leibniz Association and is funded jointly by the German federal government and a number of state governments.

DIMACS Seminar on Probabilistic Analysis of Algorithms (1997)

Seminario

The analysis of linear probing hashing with buckets

Estados Unidos

Tipo de participación: Expositor oral

Nombre de la institución promotora: DIMACS

Este es un evento por invitación organizado por la comunidad internacional de Analisis de Algoritmos (a la cual pertenezco activamente) y es la continuación de los seminarios Dagstuhl en el área.

Dagstuhl Seminar on Analysis of Algorithms (1995)

Seminario

The diagonal Poisson transform and its application to the analysis of a hashing scheme

Alemania

Tipo de participación: Expositor oral

Nombre de la institución promotora: Schloss Dagstuhl - Leibniz Center for Informatics

Los seminarios Dagstuhl, son eventos en los que se participa sólo por invitación. Un grupo de líderes mundiales en un área temática organiza uno de estos seminarios y realiza invitación a expertos y estudiantes de doctorado en dichas áreas para realizar presentaciones y realizar trabajos de investigación conjunta. Sacado de su pagina Web: Schloss Dagstuhl - Leibniz Center for Informatics (German: Schloss Dagstuhl - Leibniz-Zentrum für Informatik GmbH) is the world's premier venue for informatics. It enables the international elite, promising young researchers and practitioners alike to gather together to discuss their views and research findings. The Center promotes fundamental and applied research, continuing and advanced academic education, and the transfer of knowledge between those involved in the research side and application side of informatics. The key instrument for promoting research are the Dagstuhl Seminars, which bring together internationally renowned leading scientists for the purpose of exploring a cutting-edge informatics topic. The friendly and open climate at the conference center promotes a culture of communication and exchange among the seminar participants. The non-profit Center is a member of the Leibniz Association and is funded jointly by the German federal government and a number of state governments.

JURADO/INTEGRANTE DE COMISIONES EVALUADORAS DE TRABAJOS ACADÉMICOS

Metadata-based Provenance (2015)

Candidato: Agustín Mullin
Tipo Jurado: Tesis de Maestría
VARGAS, G. , CALEGARI, D. , VIOLA, A.
Maestría en Informática (UDELAR-PEDECIBA) / Sector Educación Superior/Público / Universidad de la República / Facultad de Ingeniería - UDeLaR / Uruguay
País: Uruguay
Idioma: Inglés
Palabras Clave: metadatos provenance
Areas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Sistemas de Información

Participación en tribunal para evaluar cargo de profesor regular asociado con dedicación semiexclusiva (2009)

Candidato: Varios Candidatos
Tipo Jurado: Otras
GORDILLO, S , MATAMALA, M , VIOLA, A.
Ingeniería / Sector Extranjero/Internacional/Otros / Institución Extranjera / Universidad de Buenos Aires / Argentina
País: Argentina
Idioma: Español
Palabras Clave: Profesor Regular Asociado
Areas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Estructuras de Datos y Algoritmos
NO encontré un lugar mejor en el CVuy para poner esta información

Analyses de l'algorithmme de Gauss. Applications a l'analyse de l'algorithmme LLL (2009)

Candidato: Antonio Vera
Tipo Jurado: Tesis de Doctorado
B. VALLÉE , FLAJOLET P. , HANROT G. , MAASA , BERTHÈ V. , DAUDÈ H. , VIOLA, A.
Doctorat Specialite: Informatique / Sector Extranjero/Internacional/Otros / Institución Extranjera / Universite de Caen / Francia
País: Francia
Idioma: Francés
Palabras Clave: Algoritmo LLL
Areas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / analisis de algoritmos

Participación en tribunal para evaluar cargo de profesor regular asociado con dedicación semiexclusiva (2008)

Candidato: Varios Candidatos
Tipo Jurado: Otras
GORDILLO, S , JOFRE, A , VIOLA, A.
Ingeniería / Sector Extranjero/Internacional/Otros / Institución Extranjera / Universidad de Buenos Aires / Argentina
País: Argentina

Idioma: Español
Palabras Clave: Profesor Regular Asociado
Áreas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Ingeniería de Software
NO encontré otro lugar en el CVuy para poner este tipo de evaluación

(2008)

Candidato: Daniel Perovich
Tipo Jurado: Tesis de Maestría
VIOLA, A.
Maestría en Informática (UDELAR-PEDECIBA) / Sector Educación Superior/Público / Universidad de la República / Facultad de Ingeniería - UDeLaR / Uruguay
País: Uruguay
Idioma: Español

(2005)

Candidato: Javier Preciozzi
Tipo Jurado: Tesis de Maestría
VIOLA, A.
Maestría en Informática (UDELAR-PEDECIBA) / Sector Educación Superior/Público / Universidad de la República / Facultad de Ingeniería - UDeLaR / Uruguay
País: Uruguay
Idioma: Español

(2004)

Candidato: Silvia Viola
Tipo Jurado: Tesis de Maestría
VIOLA, A.
Maestría en Física (UDELAR-PEDECIBA) / Sector Educación Superior/Público / Universidad de la República / Facultad de Ciencias - UDeLaR / Uruguay
País: Uruguay
Idioma: Español

(2004)

Candidato: Gabriele Facciolo
Tipo Jurado: Tesis de Maestría
VIOLA, A.
Maestría en Informática (UDELAR-PEDECIBA) / Sector Educación Superior/Público / Universidad de la República / Facultad de Ingeniería - UDeLaR / Uruguay
País: Uruguay
Idioma: Español

(2003)

Candidato: Leslie Murray
Tipo Jurado: Tesis de Maestría
VIOLA, A.
Maestría en Informática (UDELAR-PEDECIBA) / Sector Educación Superior/Público / Universidad de la República / Facultad de Ingeniería - UDeLaR / Uruguay
País: Uruguay
Idioma: Español

Información adicional

Uno de los motivos de mayor satisfacción tanto académica como personal es ver mucha gente joven exitosa en diversos lugares del mundo, quienes de diversas maneras han valorado (!) y participado de actividades científicas que he impulsado y llevado adelante. Es el motivo principal por el cual, a pesar de la gran cantidad de situaciones adversas que he tenido que soportar, sigo por el momento trabajando en el país.

Mi actividad académica ha sido el motor que ha impulsado una amistad muy profunda con una gran cantidad de investigadores dispersos en diversos laboratorios científicos de primer nivel internacional. Por tal motivo, la publicación de trabajos conjuntos, la presentación y aprobación de proyectos de investigación y colaboración conjunta, la organización de eventos internacionales, las tutorías y co-tutorías de estudiantes y las periódicas visitas académicas son un motivo de gratos

encuentros y muchas veladas que recordaremos y compartiremos toda la vida. Es claro que este vínculo tiene un impacto muy positivo en la calidad académica de nuestras publicaciones y de los estudiantes que han tomado nuestros cursos o han sido dirigidos en forma personal o en co-tutorías. Este valor agregado, es el principal motivo por el cual he podido salir adelante en mis actividades académicas en el país a pesar de todas las dificultades y contratiempos que he tenido.

Mis trabajos académicos editados, publicados y presentados incluyen coautores de los siguientes países: Argentina, Alemania, Bélgica, Canadá, Chile, China, Egipto, Eslovenia, España, Estados Unidos, Francia, Holanda, India, Inglaterra, México, Rusia, Suecia y Uruguay.

Siguiendo las indicaciones en <http://algo.inria.fr/flajolet/numbers.html>), mi número de Flajolet es 1, mi número de Erdős es 2 (<http://www.oakland.edu/~grossman/erdoshp.html>), mi número de Knuth es también 2 y mi número de Einstein es como máximo 7.

Desde 1991 a 1995 fui administrador de la primera mailing list de uruguayos que comunicó a más de 400 uruguayos en diversas partes del mundo. Muchas de las actividades de desarrollo científico - tecnológico - social, y de colaboración entre uruguayos radicados en el país y en el exterior surgieron de contactos hechos en dicha lista. La colaboración con los laboratorios HP es uno de los ejemplos más paradigmáticos.

Disfruto de los viajes y el aire libre. Son especialmente mencionables los momentos en La Floresta con mi familia, llena de niños y adolescentes, y con muchos amigos de diversas partes del mundo. Tenemos un cuaderno donde firma cada persona que se queda a dormir al menos una noche (una vez por cada estadía que haga) y en 7 años hemos coleccionado 387 firmas con gente de 18 países. Una parte importante de mi investigación científica realizada con colaboración internacional fue inspirada en este ambiente de trabajo.

En un momento tocaba guitarra, y espero retomar pronto. Como guitarrista y cantante soy un buen investigador en computación, pero me divierto.

Me gusta mucho jugar al bridge, aunque deseo de todo corazón poder jugarlo mejor!

Es un gusto asistir periódicamente a ver partidos de Defensor, tanto en el Uruguay como en el extranjero. En muchos aspectos para nada triviales, es un apostolado comparable al hacer investigación científica en Uruguay!

(28/05/2012)

Indicadores de producción

PRODUCCIÓN BIBLIOGRÁFICA	43
Artículos publicados en revistas científicas	17
Completo	17
Trabajos en eventos	21
Libros y Capítulos	5
Libro publicado	4
Capítulos de libro publicado	1
PRODUCCIÓN TÉCNICA	15
Trabajos técnicos	4
Otros tipos	11
EVALUACIONES	64
Evaluación de proyectos	7
Evaluación de eventos	43
Evaluación de publicaciones	7
Evaluación de convocatorias concursables	5
Jurado de tesis	2
FORMACIÓN RRHH	33
Tutorías/Orientaciones/Supervisiones concluidas	25
Tesis de maestría	4
Tesis/Monografía de grado	20
Tesis de doctorado	1
Tutorías/Orientaciones/Supervisiones en marcha	8
Tesis de maestría	1
Tesis de doctorado	1

