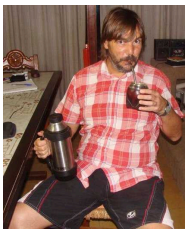

Curriculum Vitae

Alfredo VIOLA DEAMBROSIS

Actualizado: 09/11/2016

Publicado: 12/06/2017

Sistema Nacional de Investigadores

Ciencias Naturales y Exactas / Ciencias de la Computación e Información

Categorización actual: Nivel II

Ingreso al SNI: Activo(01/11/2008)

EVALUADOR ANII

Evaluador perteneciente a comité, participó en: 2007, 2008, 2009

Datos generales

Información de contacto

E-mail: viola@fing.edu.uy

Teléfono: 7114244

Dirección: Instituto de Computaciòn Facultad de Ingenierìa Julio Herrera y Reissig 565 Piso 5 CP 11.300

Institución principal

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

Dirección institucional

Dirección: Facultad de Ingeniería - UDeLaR / Instituto de Computación - Julio Herrera y Reissing 565 Piso 5 / 11300 / Montevideo / Montevideo / Uruguay

Teléfono: (+5982) 711 4244

Fax: 711 0469

E-mail/Web: viola@fing.edu.uy

Formación

Formación concluida

Formación académica/Titulación

Posgrado

1990 - 1995 Doctorado

University of Waterloo , Canadá

Título: Ph.D en Matemáticas - Opción Ciencias de la Computación

Tutor/es: James Ian Munro y Patricio Poblete

Obtención del título: 1995

Becario de: National Research Council of Canada , Canadá

Palabras clave: linear probing hashing; Diagonal Poisson Transform

Areas del conocimiento: Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Algoritmos - Análisis de Algoritmos - Combinatoria - Teoría de la Información

1988 - 1989 Maestría

University of Waterloo , Canadá

Título: Master of Mathematics

Tutor/es: Gastón Gonnet

Obtención del título: 1989

Becario de: National Research Council of Canada , Canadá

Areas del conocimiento: Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Algoritmos

Grado

1982 - 1986 Grado

Facultad de Ingeniería - UDeLaR, Universidad de la República , Uruguay

Título: Ingeniero de Sistemas en Computación

Obtención del título: 1986

Areas del conocimiento: Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Ingeniería en Computación

Construcción institucional

Colaboré sustancialmente en la construcción del Núcleo de Teoría de la Información de la Facultad de Ingeniería. Empezó en 2000 con una colaboración con el grupo de Teoría de la Información de los Laboratorios HP, California. Esta colaboración consisitió en el dictado de cursos de grado y posgrado, pasantías de estudiantes e investigadores a los Laboratorios, organización de eventos como ITW en 2006 y formación de estudiantes de Masters y Doctorado. En 2010 se creó formalmente el Núcleo de Teoría de la Información. Hoy en día estoy formando gente en Combinatoria Analítica y aplicaciones a criptografía, comunicaciones y recuperación de linformación.

Idiomas

Español

Entiende (Muy Bien) / Habla (Muy Bien) / Lee (Muy Bien) / Escribe (Muy Bien)

Francés

Entiende (Bien) / Habla (Regular) / Lee (Bien) / Escribe (Regular)

Inglés

Entiende (Muy Bien) / Habla (Muy Bien) / Lee (Muy Bien) / Escribe (Muy Bien)

Italiano

Entiende (Regular) / Habla (Regular) / Lee (Bien) / Escribe (Regular)

Portugués

Entiende (Regular) / Habla (Regular) / Lee (Bien) / Escribe (Regular)

Areas de actuación

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

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 / criptografia

Actuación Profesional

Cargos desempeñados actualmente

Desde: 03/2008

Investigador Honorario Grado 5 , (40 horas semanales) , Programa de Desarrollo de las Ciencias Básicas , Uruguay

Desde: 02/2003

Instituto de Computación , (Docente Grado 5 Titular, 40 horas semanales / Dedicación total) , Facultad de Ingeniería - UDeLaR , Uruguay

Desde: 06/2015

(40 horas semanales) , Universite de Paris VIII , Francia

Programa de Desarrollo de las Ciencias Básicas , Programa de Desarrollo de las Ciencias Básicas , Uruguay

Vínculos con la institución

03/2008 - Actual, *Vínculo:* Investigador Honorario Grado 5, (40 horas semanales)

03/2001 - 03/2008, *Vínculo:* Investigador Honorario Grado 4, (40 horas semanales)

03/1996 - 03/2001, *Vínculo:* Investigador Honorario Grado 3, (40 horas semanales)

Actividades

03/1999 - Actual

Gestión Académica

Miembro del Consejo Científico del área de Informática

03/2009 - 03/2011

Gestión Académica

Delegado de los investigadores a la Comisión Directiva del Pedeciba.

03/2006 - 12/2007

Gestión Académica

Coordinador del Area de Informática del Pedeciba

07/1997 - 07/2007

Gestión Académica

Miembro de la Comisión de Posgrado del Area de Informática

03/2001 - 03/2003

Gestión Académica

Coordinador Titular y luego Coordinador Alterno del Pedeciba Informática

Universidad de la República , Facultad de Ingeniería - UDeLaR , Uruguay

Vínculos con la institución

02/2003 - Actual, *Vínculo:* Instituto de Computación, Docente Grado 5 Titular, (40 horas semanales / Dedicación total)

08/1996 - 02/2003, *Vínculo:* Instituto de Computación, Docente Grado 4 Titular, (40 horas semanales)

03/1986 - 06/1990, *Vínculo:* Instituto de Computación, Docente Grado 2 Interino, (30 horas semanales)

08/1986 - 09/1987, *Vínculo:* IMERL, Docente Grado 1 Interino, (10 horas semanales)

03/1982 - 12/1985, *Vínculo:* Cátedra de Matemática I - Ciencias Económicas, Docente Grado 1 Interino, (12 horas semanales)

07/1990 - 07/1996, *Vínculo:* , Docente Grado 4 Titular, (40 horas semanales)

Actividades

01/2006 - Actual

Líneas de Investigación

Manejo de información en redes globales , Integrante del Equipo

01/2006 - Actual

Líneas de Investigación

Bioinformática , Coordinador o Responsable

01/2001 - Actual

Líneas de Investigación

Teoría de la Información , Coordinador o Responsable

03/1998 - Actual

Líneas de Investigación

Criptografía , Coordinador o Responsable

01/1997 - Actual

Líneas de Investigación

Análisis de Algoritmos - Combinatoria , Coordinador o Responsable

06/2015 - Actual

Docencia , Grado

Programación 3 , Asistente , Ingeniería en Computación

02/2013 - Actual

Docencia , Grado

Combinatoria Analítica , Responsable , Ingeniería en Computación

02/2013 - Actual

Docencia , Grado

Teoría de la Computación , Responsable , Ingeniería en Computación

01/1997 - 12/2002

Docencia , Grado

Programación 3 , Ingeniería en Computación

01/1987 - 06/1988

Docencia , Grado

Ayudante del curso de Probabilidad y Estadística , Ingeniería Eléctrica

03/1986 - 06/1988

Docencia , Grado

Programación III (Plan 85) , Ingeniería en Computación

03/1986 - 06/1988

Docencia , Grado

Programacion II (Plan 85) , Ingeniería en Computación

09/2012 - Actual

Docencia , Maestría

Fundamentos de Criptografía , Responsable , Maestría en Seguridad Informática

01/1997 - Actual

Docencia , Maestría

Análisis de Algoritmos , Maestría en Informática (UDELAR-PEDECIBA)

01/1997 - Actual

Docencia , Maestría

Criptograía , Maestría en Informática (UDELAR-PEDECIBA)

01/1997 - Actual

Docencia , Maestría

Teoría de Códigos , Maestría en Informática (UDELAR-PEDECIBA)

01/1997 - Actual

Docencia , Doctorado

Análisis de Algoritmos , Doctorado en Informática (UDELAR-PEDECIBA)

01/1997 - Actual

Docencia , Doctorado

Teoría de Códigos , Doctorado en Informática (UDELAR-PEDECIBA)

01/1997 - Actual

Docencia , Doctorado

Criptograía , Doctorado en Informática (UDELAR-PEDECIBA)

06/2010 - Actual

Extensión , PEDECIBA/Plan Ceibal

Científicos en el Aula

02/2005 - Actual

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)

06/2001 - 06/2004

Extensión

Asesoramiento al Gobierno Nacional en temas relacionados con comercio electrónico

03/2000 - 06/2002

Extensión

Asesoramiento al Parlamento Nacional en relacion a leyes sobre comercio electronico (colaboracion con Facultad de Derecho)

02/2015 - Actual

Gestión Académica

Miembro suplente de comisión de instituto de computación

11/2014 - Actual

Gestión Académica

Miembro de la comisión de enseñanza del Claustro

11/2014 - Actual

Gestión Académica , Facultad de Ingeniería , Instituto de Computación

Miembro suplente de la Comisión de Instituto

01/1997 - Actual

Gestión Académica

Director del grupo de investigación de Algoritmos y Análisis de Algoritmos

08/2005 - 09/2014

Gestión Académica

Miembro Alterno de la Comisión Academica de Posgrado de la Facultad de Ingeniería

09/2006 - 06/2014

Gestión Académica

Consejero Titular de Facultad de Ingeniería

03/2004 - 07/2008

Gestión Académica

Miembro del Consejo Académico del Instituto de Computación

07/1997 - 07/2008

Gestión Académica

Miembro de la Subcomision Académica de Posgrado de Ingeniería en Computación

09/2004 - 09/2006

Gestión Académica

Miembro de la directiva de ADFI

09/2000 - 09/2004

Gestión Académica

Miembro de la Comisión de Posgrado del Claustro de la Facultad de Ingeniería

09/2000 - 09/2004

Gestión Académica

Miembro Titular del Claustro de la Facultad de Ingeniería

03/2000 - 03/2001

Gestión Académica

Ejercicio de dirección del Instituto de Computación en ausencia del director Raúl Ruggia.

12/2015 - Actual

Proyectos de Investigación y Desarrollo , STIC-AMSUD

AleaEnAmSud (Proyecto STIC-AMSUD) , Coordinador o Responsable

04/2015 - Actual

Proyectos de Investigación y Desarrollo , Universidad de la República , CSIC I+D

Combinatoria Analítica y Aplicaciones , Coordinador o Responsable

01/2015 - Actual

Proyectos de Investigación y Desarrollo , Universidad de Chile , Red internacional sobre voto electrónico

Red internacional sobre voto electrónico , Integrante del Equipo

01/2013 - 01/2014

Proyectos de Investigación y Desarrollo , STIC-AMSUD

DYNALCO: Advances in Analytic Combinatorics: dynamical combinatorics, and applications to number theory, information theory and cryptography. , Coordinador o Responsable

07/2010 - 07/2013

Proyectos de Investigación y Desarrollo , ANR Project BOOLE; ANR-09-BLAN-0011

Boole , Otros/investigador invitado

09/2008 - 10/2012

Proyectos de Investigación y Desarrollo

JARDIN: Just an Assistant foR Instructional DesiIgN , Integrante del Equipo

02/2009 - 02/2012

Proyectos de Investigación y Desarrollo , ECOS

Estudio cuantitativo de clases de estructuras combinatorias y sus aplicaciones en criptografía y Teoría de la Información , Coordinador o Responsable

04/2009 - 06/2011

Proyectos de Investigación y Desarrollo , STIC-AMSUD

FMCrypto: Formal Methods for Cryptographically Secure Distributed Computations , Integrante del Equipo

04/2009 - 06/2011

Proyectos de Investigación y Desarrollo , CSIC

Análisis de Funciones Booleanas y sus Aplicaciones a la Criptografía , Coordinador o Responsable

03/2006 - 05/2008

Proyectos de Investigación y Desarrollo

Codigos libres de prefijos óptimos con alfabetos infinitos y su uso en algoritmos eficientes de compresión , Coordinador o Responsable

03/2005 - 03/2007

Proyectos de Investigación y Desarrollo

Estudio de Modelos para procesos estocásticos de memoria finita , Coordinador o Responsable

03/2002 - 03/2004

Proyectos de Investigación y Desarrollo

Diseño, análisis e implementación de diversos algoritmos de almacenamiento, búsqueda y recuperación de información , Coordinador o Responsable

03/2000 - 03/2002

Proyectos de Investigación y Desarrollo

Desarrollo de métodos matemáticos para analizar algoritmos y su aplicación al análisis de algoritmos criptográficos

03/1997 - 03/1999

Proyectos de Investigación y Desarrollo

Manejo de información en redes globales , Coordinador o Responsable

Universite de Paris XIII (Paris-Nord) , Universite de Paris XIII (Paris-Nord) , Francia

Vínculos con la institución

11/2003 - 11/2010, *Vínculo:* Profesor Asociado, (1 horas semanales)

06/2003 - 11/2003, *Vínculo:* Poste Rouge CNRS, (40 horas semanales / Dedicación total)

05/2006 - 06/2006, *Vínculo:* , (40 horas semanales)

05/2010 - 05/2010, *Vínculo:* , (40 horas semanales)

Universidad de Chile , Chile

Vínculos con la institución

12/1997 - 12/1997, *Vínculo:* , (40 horas semanales)

12/1996 - 12/1996, *Vínculo:* , (40 horas semanales)

12/1998 - 12/1998, *Vínculo:* , (40 horas semanales)

12/1999 - 12/1999, *Vínculo:* , (40 horas semanales)

12/2000 - 12/2000, *Vínculo:* , (40 horas semanales)

12/2006 - 12/2006, *Vínculo:* , (40 horas semanales)

12/2007 - 12/2007, *Vínculo:* , (40 horas semanales)

12/2009 - 12/2009, *Vínculo:* , (40 horas semanales)

12/2012 - 12/2012, *Vínculo:* , (40 horas semanales)

University of Waterloo , University of Waterloo , Canadá

Vínculos con la institución

09/1996 - 09/1996, *Vínculo:* , (40 horas semanales)

05/1997 - 06/1997, *Vínculo:* , (40 horas semanales)

06/2001 - 06/2001, *Vínculo:* , (40 horas semanales)

01/1989 - 07/1995, *Vínculo:* Teacher Assistant, (5 horas semanales)

07/2015 - 07/2015, *Vínculo:* , (40 horas semanales)

Carleton University , Canadá

Vínculos con la institución

06/2001 - 06/2001, *Vínculo:* , (40 horas semanales)

07/2002 - 07/2002, *Vínculo:* , (40 horas semanales)

04/2004 - 04/2004, *Vínculo:* , (40 horas semanales)

05/2009 - 05/2009, *Vínculo:* , (40 horas semanales)

Institut National de Recherche en Informatique et Automatique , Francia

Vínculos con la institución

06/2002 - 06/2002, *Vínculo:* , (40 horas semanales)

06/2007 - 06/2007, *Vínculo:* , (40 horas semanales)

Université de Marne la Vallée , Francia

Vínculos con la institución

05/2005 - 06/2005, *Vínculo:* , (40 horas semanales)

07/2007 - 07/2007, *Vínculo:* , (40 horas semanales)

07/2008 - 07/2008, *Vínculo:* , (40 horas semanales)

Hewlett-Packard Laboratories , Estados Unidos

Vínculos con la institución

01/2002 - 01/2002, *Vínculo:* , (40 horas semanales)

06/2004 - 06/2004, *Vínculo:* , (40 horas semanales)

01/2007 - 01/2007, *Vínculo:* , (40 horas semanales)

Universitat Bonn , Alemania

Vínculos con la institución

07/2007 - 07/2007, *Vínculo:* , (20 horas semanales)

06/2010 - 06/2010, *Vínculo:* , (40 horas semanales)

Universite de Caen , Francia

Vínculos con la institución

06/2007 - 06/2007, *Vínculo:* , (40 horas semanales)

06/2008 - 07/2008, *Vínculo:* , (40 horas semanales)

07/2009 - 07/2009, *Vínculo:* , (40 horas semanales)

06/2010 - 07/2010, *Vínculo:* , (40 horas semanales)

06/2013 - 06/2013, *Vínculo:* , (40 horas semanales)

06/2014 - 06/2014, *Vínculo:* , (40 horas semanales)

06/2015 - 06/2015, Vínculo: , (40 horas semanales)

Universidad Politécnica de Catalunya* , España

Vínculos con la institución

07/2008 - 07/2008, *Vínculo:* , (40 horas semanales)

04/2004 - 04/2004, *Vínculo:* , (40 horas semanales)

07/2001 - 07/2001, *Vínculo:* , (40 horas semanales)

11/2000 - 11/2000, *Vínculo:* , (40 horas semanales)

07/1997 - 07/1997, *Vínculo:* , (40 horas semanales)

06/2009 - 06/2009, *Vínculo:* , (40 horas semanales)

09/2011 - 08/2012, *Vínculo:* Año sabàtico, (40 horas semanales)

05/2013 - 06/2013, *Vínculo:* , (40 horas semanales)

06/2014 - 06/2014, *Vínculo:* , (40 horas semanales)

05/2015 - 06/2015, *Vínculo:* , (40 horas semanales)

Actividades

07/2001 - 07/2011

Docencia , Doctorado

Anàlisis de algoritmos de ordenaciòn y bùsqueda , Invitado

06/2009 - 06/2009

Docencia , Doctorado

Introducciòn a la Teorìa de Còdigos

07/2008 - 07/2008

Docencia , Doctorado

Introducciòn a la Teorìa de Còdigos , Invitado

Universidad Estadual de Campinas , Brasil

Vínculos con la institución

05/2009 - 05/2009, *Vínculo:* , (40 horas semanales)

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

Vínculos con la institución

05/2010 - 05/2010, *Vínculo:* , (40 horas semanales)

Universite de Paris VIII , Universite de Paris VIII , Francia

Vínculos con la institución

06/2015 - Actual, *Vínculo:* , (40 horas semanales)

Lineas de investigación

Título: Análisis de Algoritmos - Combinatoria

Tipo de participación: Coordinador o Responsable

Objetivo: Desarrollo y utlización de herramientas analítico-combinatorias para analizar el comportamiento prácitco 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 cientícos 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-tecnoloógicos 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.

Equipos: Alvaro Martín(Integrante); Fernando Fernández(Integrante)

Areas del 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 / combinatoria

Título: Bioinformática

Tipo de participación: Coordinador o Responsable

Objetivo: 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 consolidad algún trabajo en 2009, que pueda vincular algun proyecto de grado con estudiantes de informática. Esta es una línea nueva y tentativa de investigación conjunta, que si bien es muy promisoria, aún no hemos logrado concretar ningun proyecto conjunto. Esperamos poder dar avances en esta dirección en 2009.

Areas del conocimiento: Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / bioinformática

Título: Criptografía

Tipo de participación: Coordinador o Responsable

Objetivo: 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, oprtando 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 Intormation 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 Informatica del Instituto de Computación dirigido por el Dr. Gustavo Betarte.

Equipos: Alvaro Martín(Integrante); Fernando Fernández(Integrante); Nicolás Carrasco(Integrante); Matías Hernández(Integrante)

Areas del conocimiento: Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / criptografia

Título: Manejo de información en redes globales

Tipo de participación: Integrante del Equipo

Objetivo: 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.

Areas del conocimiento: Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / almacenamiento y recuperación de informacion
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

Título: Teoría de la Información

Tipo de participación: Coordinador o Responsable

Objetivo: 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 esutdiantes 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.

Equipos: Alvaro Martín(Integrante); Fernando Fernández(Integrante); Nicolás Carrasco(Integrante); Matías Hernández(Integrante)

Areas del conocimiento: Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Teoría de la Información

Proyectos

2015 - Actual

Título: AleaEnAmSud (Proyecto STIC-AMSUD), *Tipo de participación:* Coordinador o Responsable, *Descripción:* Proyecto STIC-AMSUD con participación de investigadores de la Universidad de Caen y Paris 7 (Francia) y de la Universidad Nacional General Sarmiento (Argentina).

Tipo: Investigación

Alumnos: 2(Pregrado), 1(Doctorado)

Financiadores: Agencia Nacional de Investigación e Innovación / Cooperación

Palabras clave: Análisis dinámico de algoritmos; Combinatoria; criptografía

Areas del conocimiento: Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Análisis Dinámico de Algoritmos

2015 - Actual

Título: Combinatoria Analítica y Aplicaciones, *Tipo de participación:* Coordinador o Responsable, *Descripción:* Proyecto de Investigación CSIC con la participación de 2 estudiantes de grado, 1 estudiante de Maestría y un estudiante interesado en ingresar al doctorado.

Tipo: Investigación

Alumnos: 2(Pregrado), 1(Maestría/Magister), 1(Doctorado)

Equipo: Adrián Silveira(Integrante); Sebastián Fonseca(Integrante); Pablo Rotondo(Integrante)

Palabras clave: Combinatoria Analítica

2015 - Actual

Título: Red internacional sobre voto electrónico, *Tipo de participación:* Integrante del Equipo, *Descripción:* Red de colaboración con científicos chilenos y franceses financiado por el INRIA-Chile.

Tipo: Investigación

Alumnos:

Palabras clave: Voto Electrónico

1997 - 1999
Título: Manejo de información en redes globales, *Tipo de participación:* Coordinador o Responsable, *Descripción:* Fondo Clemente Estable
Tipo: Desarrollo

Alumnos: 8(Pregrado),

Financiadores: DINACYT/DICYT/CONICYT / Apoyo financiero

2000 - 2002
Título: Desarrollo de métodos matemáticos para analizar algoritmos y su aplicación al análisis de algoritmos criptográficos, *Descripción:* Proyecto en colaboración con investigadores de Chile y de Canadá.
Tipo: Investigación

Alumnos: 4(Pregrado),

Equipo: Daniel Panario(Integrante); Patricio Poblete(Integrante)

Financiadores: Comisión Sectorial de Investigación Científica - UDeLaR / Apoyo financiero

2002 - 2004
Título: Diseño, análisis e implementación de diversos algoritmos de almacenamiento, búsqueda y recuperación de información, *Tipo de participación:* Coordinador o Responsable, *Descripción:* Proyecto con colaboración de investigadores de Canadá y España.

Tipo: Desarrollo

Alumnos: 1(Pregrado),

Equipo: Daniel Panario(Integrante); Conrado Martínez(Integrante)

Financiadores: Comisión Sectorial de Investigación Científica - UDeLaR / Apoyo financiero

2005 - 2007
Título: Estudio de Modelos para procesos estocásticos de memoria finita, *Tipo de participación:* Coordinador o Responsable, *Descripción:* Proyecto CSIC con colaboración de investigadores de los laboratorios HP en California.
Tipo: Desarrollo

Alumnos: 1(Doctorado)

Equipo: Gadiel Seroussi(Integrante); Marcelo Weinberger(Integrante)

Financiadores: Comisión Sectorial de Investigación Científica - UDeLaR / Apoyo financiero

2006 - 2008
Título: Codigos libres de prefijos óptimos con alfabetos infinitos y su uso en algoritmos eficientes de compresión, *Tipo de participación:* Coordinador o Responsable, *Descripción:* Proyecto PDT, con participación de investigadores de Francia y de los laboratorios HP, California
Tipo: Investigación

Alumnos: 1(Maestría/Magister),
Equipo: Fernando Fernández(Integrante); Gadiel Seroussi(Integrante); Frédérique Bassino(Integrante); Julien Clément(Integrante); Alfredo Viola(Responsable)
Financiadores: DINACYT/DICYT/CONICYT / Apoyo financiero

2009 - 2011
Título: Análisis de Funciones Booleanas y sus Aplicaciones a la Criptografía, *Tipo de participación:* Coordinador o Responsable, *Descripción:* Proyecto de Investigación CSIC en conjunto con investigadores de las Universidades de Caen y Paris XIII (Francia)

Tipo: Investigación

Alumnos: 1(Pregrado), 1(Maestría/Magister),
Equipo: Nicolás Carrasco(Integrante); Matías Hernández(Integrante); Gadiel Seroussi(Integrante); Frédérique Bassino(Integrante); Julien Clément(Integrante)
Financiadores: Comisión Sectorial de Investigación Científica - UDeLaR / Apoyo financiero

Palabras clave: funciones booleanas; criptografía
Areas del 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 / criptografia
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Teoría de la Información

2009 - 2011

Título: FMCrypto: Formal Methods for Cryptographically Secure Distributed Computations , *Tipo de participación:* Integrante del Equipo, *Descripción:* Programa de cooperación STIC-AMSUD con investigadores de Francia, Brasil y Chile. The overall goal t 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.

Tipo: Investigación

Alumnos: 1(Pregrado), 1(Maestría/Magister),

Equipo: Matías Hernández(Integrante); Gustavo Betarte(Integrante); Carlos Luna(Integrante); Felipe Zipitría(Integrante); Tamara Rezk(Responsable); Ricardo Dahab(Integrante); Alejandro Hevia(Integrante)

Financiadores: Agencia Nacional de Investigación e Innovación / Apoyo financiero

Palabras clave: criptografía; seguridad de la información

Areas del conocimiento: Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / criptografia

2009 - 2012

Título: Estudio cuantitativo de clases de estructuras combinatorias y sus aplicaciones en criptografía y Teoría de la Información, *Tipo de participación:* Coordinador o Responsable, *Descripción:* Programa ECOS de cooperación francesa con la Universidad de París XIII y la Universidad de Caen

Tipo: Investigación

Alumnos: 1(Pregrado), 1(Maestría/Magister),

Equipo: Nicolás Carrasco(Integrante); Matías Hernández(Integrante); Gadiel Seroussi(Integrante); Frédérique Bassino(Integrante); Julien Clément(Integrante); Brigitte Vallée(Integrante)

Financiadores: Otra institución nacional / Universidad de la República - Proyecto ECOS - Cooperación internacional / Apoyo financiero

Palabras clave: funciones booleanas; criptografía; Combinatoria; Teoría de la Información

Areas del conocimiento: Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / criptografia

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

2008 - 2012

Título: JARDIN: Just an Assistant foR Instructional DesiIgN, *Tipo de participación:* Integrante del Equipo, *Descripción:* Proyecto financiado por LACCIR (red latinoamericana impulsada por Microsoft), dirigido por Regina Motz (Universidad de la República, Uruguay) y con participacion de miembros de 6 países.

Tipo: Investigación

Alumnos: 2(Pregrado), 1(Maestría/Magister),

Equipo: Regina Motz(Responsable)

Financiadores: Institución del exterior / Microsoft / Apoyo financiero

2010 - 2013

Título: Boole, *Tipo de participación:* Otros/investigador invitado, *Descripción:* 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 dato tambien varias charlas.

Tipo: Investigación

Alumnos:

Equipo: Alfredo(Integrante)

Financiadores: Institución del exterior / ANR (Francia) / Apoyo financiero

Palabras clave: funciones booleanas

Areas del conocimiento: Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / combinatoria analítica

2013 - 2014

Título: DYNALCO: Advances in Analytic Combinatorics: dynamical combinatorics, and applications to number theory, information theory and cryptography., *Tipo de participación:* Coordinador o Responsable, *Descripción:* 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.

Tipo: Desarrollo

Alumnos: 1(Pregrado), 2(Maestría/Magister),

Equipo: Nicolás(Integrante); Fernando(Integrante); Sebastián(Integrante)

Financiadores: Agencia Nacional de Investigación e Innovación / Cooperación

Palabras clave: Análisis de Algoritmos; sistemas dinámicos

Areas del conocimiento: Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / combinatoria analítica

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 volúmen 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 construír 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.

Sistema Nacional de Investigadores

Producción bibliográfica

Artículos publicados

Arbitrados

Completo

SVANTE JANSON; VIOLA, A.

A unified approach to linear probing hashing (aceptado en número especial para trabajos seleccionados AofA2014). Algorithmica, v.: 75, p.: 1 - 58, 2016

Palabras clave: *hashing*

Areas del 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.


Completo

P. POBLETE; VIOLA, A.

Analysis of Robin Hood and other hashing algorithms under the random probing model, with and without deletions. Combinatorics Probability and Computing (E), 2016

Palabras clave: hashing

Areas del conocimiento: Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / analisis de algoritmos

ISSN: 14692163

Completo

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

Optimal prefix codes for pairs of geometrically-distributed random variables . IEEE Transactions on Information Theory, *v.:* 59 4, *p.:* 2375 - 2395, 2013

Palabras clave: Códigos de prefijos óptimos; alfabetos infinitos; distribución geométrica bidimensional

Areas del 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


Completo

GATHEN J.; ZIEGLER K.; VIOLA, A.

Counting reducible, squareful, and relatively irreducible multivariate polynomials over finite fields. SIAM Journal on Discrete Mathematics, *v.:* 27 2, *p.:* 855 - 891, 2013

Areas del 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 / cuerpos finitos

ISSN: 08954801


Completo

N. CARRASCO; LE BARS J.M.; VIOLA, A.

Enumerative Encoding of first order correlation immune Boolean Functions. Theoretical Computer Science, *v.:* 487, *p.:* 23 - 36, 2013

Palabras clave: Resilient Functions; Enumerative Coding

Areas del conocimiento: Ingeniería y Tecnología / Ingeniería Eléctrica, Ingeniería Electrónica e Ingeniería de la Información / Telecomunicaciones / Boolean Functions

ISSN: 03043975


Completo

A. HEVIA; P. POBLETE; VIOLA, A.
Efficiency of Anonymous Cryptographic Communication with DC Nets (En preparación). Theoretical Computer Science, 2011

Palabras clave: DC Nets

Areas del conocimiento: Ciencias Naturales y Exactas / Matemáticas / Matemática Aplicada / Criptografía
Ciencias Naturales y Exactas / Matemáticas / Matemática Aplicada / Combinatoria

ISSN: 03043975

THOMSON ISI SCOPUS

Completo

DEVROYE, L; VIOLA, A.
Maximal Displacement in Linear Probing Hashing with a Robin Hood Protocol (EN Preparación). Information Processing Letters, 2011

Palabras clave: Longest Probe; linear probing hashing
Areas del conocimiento: Ciencias Naturales y Exactas / Matemáticas / Matemática Aplicada / Probabilistic Analysis of Algorithms

ISSN: 00200190

Completo

D. VERGNAUD; VIOLA, A.
How to achieve the security of MACs via Randomized Message Preprocessing (en preparación). Finite Fields and their Applications, 2011

Palabras clave: polynomials over finite fields
Areas del conocimiento: Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / criptografia
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / cuerpos finitos
ISSN: 10715797

THOMSON ISI SCOPUS

Completo

LE BARS, J. M.; VIOLA, A.
Equivalence classes of boolean functions for first-order correlation . IEEE Transactions on Information Theory, *v.:* 56 3, *p.:* 1247 - 1261, 2010
Palabras clave: funciones inmunes a la correlación; funciones booleanas 1-resilientes
Areas del conocimiento: Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Funciones booleanas, criptografía
Medio de divulgación: Papel ; *ISSN:* 00189448

Completo

MARTÍNEZ, C; PANARIO, D; VIOLA, A.

Adaptive Sampling Strategies for Quickselect . ACM Transactions on Algorithms, *v.:* 6 3, 2010

Palabras clave: algoritmos de seleccion
Areas del 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/

THOMSON ISI SCOPUS

Completo

VIOLA, A.

Distributional Analysis of the Parking Problem and Robin Hood Linear Probing Hashing with Buckets - Número especial dedicado a los 60 años de Philippe Flajolet - . Discrete Mathematics and Theoretical Computer Science (DMTCS), v.: 12 2, p.: 307 - 332, 2010

Palabras clave: linear probing hashing with buckets; Parking Problem

Areas del conocimiento: Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / analisis de algoritmos

ISSN: 13658050

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 distribucion del 'Bucket occupanxy', 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'.

Completo

VIOLA, A.

Exact distribution of individual displacements in linear probing hashing. ACM Transactions on Algorithms, v.: 1 2, p.: 214 - 242, 2005

Palabras clave: linear probing hashing; Exact Distribution

Areas del 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/

Completo

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

On worst case Robin Hood Hashing . SIAM Journal on Computing, *v.:* 33 4, *p.:* 923 - 936, 2004

Palabras clave: Robin Hood Hashing

Areas del 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

Completo

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

Analysis of Rabin`s Irreducibility Test for Polynomials over Finite Fields. Random Structures Algorithms, *v.:* 19 3-4, *p.:* 525 - 551, 2001

Palabras clave: polinomios sobre cuerpos finitos

Areas del 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 / criptografia

Medio de divulgación: Papel ; *ISSN:* 10429832

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

Completo

VIOLA, A.; POBLETE, P

Analysis of Linear Probing Hashing with Buckets. Algorithmica, *v.:* 21 1, *p.:* 37 - 71, 1998

Palabras clave: linear probing hashing with buckets

Areas del 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.

THOMSON ISI SCOPUS

Completo

FLAJOLET, P; POBLETE, P; VIOLA, A.

On the Analysis of Linear Probing Hashing. Algorithmica, v.: 22 4, p.: 490 - 515, 1998

Palabras clave: linear probing hashing

Areas del 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/algorithmica22.html

THOMSON ISI SCOPUS

Completo

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

The diagonal Poisson transform and its application to the analysis of a hashing scheme. Random Structures Algorithms, *v.:* 10 2, *p.:* 221 - 255, 1997

Palabras clave: linear probing hashing; Diagonal Poisson Transform

Areas del conocimiento: Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / analisis de algoritmos

Medio de divulgación: Papel ; *ISSN:* 10429832 ; *Idioma/Pais:* Inglés/

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

THOMSON ISI SCOPUS

Artículos aceptados

Libros

Libro compilado , Revista

VIOLA, A.

Selected papers LATIN 2014. 2015. *Número de volúmenes:* 200, *Nro. de páginas:* 300,

Palabras clave: Teoría de la Computación

Areas del conocimiento: Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Teoría de la Computación

Financiación/Cooperación: Facultad de Ingeniería - UDeLaR / Otra

Libro compilado , Libro

PARDO, A.; VIOLA, A.

Proceedings LATIN 2014. 2014. *Número de volúmenes:* 150, *Nro. de páginas:* 767,

Palabras clave: Teoría de la Computación

Areas del conocimiento: Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación

Libro compilado , Libro

LóPEZ-ORTIZ, A.; BRODNIK,A; RAMAN,V; VIOLA, A.

Space-Efficient Data Structures, Streams and Algorithms (papers in honor of J. Ian Munro on the occasion of his 66th birthday). 2013. *Número de volúmenes:* 150, *Nro. de páginas:* 362, *Edicion:* 8066,

Editorial: LNCS - SPRINGER

Palabras clave: Algorithms

Areas del conocimiento: Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación

Libro compilado , Compilación

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

Proceedings LATIN 2000. 2000. *Número de volúmenes:* 150, *Nro. de páginas:* 484, *Edicion:* 1776,

Editorial: LNCS - SPRINGER

Palabras clave: Teoría de la Computación

Areas del conocimiento: Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación

ISSN/ISBN: 3540673067;

Capitulos de Libro

Capítulo de libro publicado

VIOLA, A.

Introduction to the chapter «Philippe Flajolet and his contribution to the analysis of hashing problems«. , 2013

Libro: Philippe Flajolet's collected works (7 volumes). *p.:* 355 - 360,

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

Palabras clave: hashing

Areas del conocimiento: Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / combinatoria analítica

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 pidio a varios editores que nos encargáramos de presentar ciertos capítulos. A mi me toco presentar el capítulo sobre hashing, dado que he tenido trabajos conjuntos con Philippe Flajolet.

Trabajos en eventos

Resumen expandido

P. POBLETE; VIOLA, A.

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

Evento: Internacional , 27th International Conference on Probabilistic, Combinatorial and Asymptotic Methods for the Analysis of Algorithms (AOFA 2016) , Cracovia, Polonia , 2016

Anales/Proceedings: Arbitrado: SI

Palabras clave: Robin Hood Hashing

Areas del conocimiento: Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / analisis de algoritmos

Medio de divulgación: Internet;

Financiación/Cooperación: Comisión Sectorial de Investigación Científica - UDeLaR / Apoyo financiero

https://arxiv.org/submit/1559349

Financiado por proyecto CSIC: 'Combinatoria Analítica y aplicaciones a Criptografía, Comunicaciones y Recuperación de la Información.

Resumen expandido

BERTHÈ V.; CESARATTO, E.; ROTNDO, P.; B. VALLÉE; VIOLA, A.

Recurrence function on Sturmian words: a probabilistic study , 2015

Evento: Internacional , Mathematical Foundations of Computer Science , Milán , 2015

Anales/Proceedings: Mathematical Foundations of Computer ScienceArbitrado: SI

Palabras clave: Análisis dinámico de algoritmos

Areas del conocimiento: Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / combinatoria analítica

Medio de divulgación: Internet;

Financiación/Cooperación: Facultad de Ingeniería - UDeLaR / Otra

http://mfcs2015.di.unimi.it/

Resumen expandido

SVANTE JANSON; VIOLA, A.

A unified approach to linear probing hashing , 2014

Evento: Internacional , AofA 2014 , París , 2014

Anales/Proceedings: Arbitrado: SI

Palabras clave: linear probing hashing

Areas del conocimiento: Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / combinatoria analítica

Resumen expandido

GARCÍA, P.; VAN DE GRAAF, J.; A. HEVIA; VIOLA, A.

Beating the Birthday Paradox in Dining Cryptographer Networks , 2014

Evento: Internacional , LATINCRYPT 2014 , Florianópolis , 2014

Anales/Proceedings: Arbitrado: SI

Palabras clave: DC Nets

Areas del conocimiento: Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / criptografia

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

Financiación/Cooperación: Facultad de Ingeniería - UDeLaR / Remuneración

Resumen expandido

HELMI, A.; LUMBROSO, J.; C. MARTÍNEZ; VIOLA, A.

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

Evento: Internacional , 23rd international meeting on probabilistic, combinatorial and asymptotic methods for the analysis of algorithms (AofA 2012) , Montreal, Canadá , 2012

Palabras clave: data streamming; hiring problem; distinct elements estimation

Areas del 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

Resumen expandido

N. CARRASCO; LE BARS J.M.; VIOLA, A.

Enumerative encoding of correlation immune Boolean functions , 2011

Evento: Internacional , IEEE Information Theory Workshop , Paraty, Brasil , 2011

Anales/Proceedings: Arbitrado: SI

Palabras clave: Resilient Boolean Functions; Enumerative Encoding

Areas del 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

Resumen expandido

GATHEN J.; VIOLA, A.; ZIEGLER K.

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

Evento: Internacional , LATIN 2010 , Oaxaca, Mexico , 2010

Anales/Proceedings: Arbitrado: SI

Palabras clave: polinomios sobre cuerpos finitos

Areas del 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

Resumen expandido

F. FERNÁNDEZ; VIOLA, A.; M WEINBERGER

Efficient algorithms for constructing bi-directional context sets , 2010

Evento: Internacional , IEEE Data Compression Conference , 2010

Palabras clave: context sets

Areas del 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 / Teoria de la Información

Completo

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

Equivalence classes of boolean functions for first-order correlation , 2007

Evento: Internacional , IEEE International Symposium on Information Theory , 2007

Palabras clave: funciones booleanas 1-resiliente

Areas del conocimiento: Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / criptografia

Medio de divulgación: Papel;

Completo

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

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

Evento: Internacional , ISIT - IEEE International Symposium of Information Theory , 2006

Palabras clave: Códigos de prefijos óptimos

Areas del conocimiento: Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Teoría de la Información

Medio de divulgación: Papel;

Completo

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

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

Evento: Internacional , DCC - IEEE Data Compression Conference , 2006

Palabras clave: Códigos de prefijos óptimos

Areas del conocimiento: Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Teoría de la Información

Medio de divulgación: Papel;

Completo

VIOLA, A.

Distributional Analysis of Robin Hood Linear Probing Hashing with Buckets , 2005

Evento: Internacional , First International Conference on Analysis of Algorithms , 2005

Palabras clave: linear probing hashing with buckets; Exact Distribution

Areas del conocimiento: Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / analisis 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 maximo de 50) aparecido en la primera edición del volumen 3 de 'The Art of Computer Programming' de D. Knuth (el libro mas vendido y usado en la historia de la computacion) sino que además encuentro

una solución más general. Este problema está relacionado con 'Linear Probing Hashing', que fue el primer analisis realizado por D. Knuth y que lo inspiro a escribir esta clasica coleccion de libros. En el problema se pedia 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 >=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.

Completo

MARTÍNEZ, C; PANARIO, D; VIOLA, A.

Adaptive Sampling Strategies for Quickselect , 2004

Evento: Internacional , ACM Symposium on Discrete Algorithms - SODA , 2004

Palabras clave: algoritmos de seleccion
Areas del conocimiento: Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / analisis de algoritmos
Medio de divulgación: Papel;

Completo

MARTÍNEZ, C; PANARIO, D; VIOLA, A.

Analysis of Quickfind with small subfiles , 2002
Evento: Internacional , Colloquium on Mathematics and Computer Science: Algorithms, Trees, Combinatorics and Probabilities , Versailles , 2002

Palabras clave: algoritmos de seleccion
Areas del conocimiento: Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / analisis de algoritmos
Medio de divulgación: Papel;

Completo

POBLETE, P; VIOLA, A.

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

Evento: Internacional , First Brazilian Symposium on Graphs, Algorithms and Combinatorics - GRACO , 2001

Anales/Proceedings: Electronic Notes in Discrete Mathematics , 7

Palabras clave: Hashing Algorithms; Deletions
Areas del conocimiento: Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / analisis de algoritmos
Medio de divulgación: Papel;

Completo

PANARIO, D; VIOLA, A.

Average Case Analysis of Rabin`s Irreducibility Test Algorithm , 1998

Evento: Internacional , Tercer Latin American symposium on Theoretical Informatics , 1998

Anales/Proceedings: Lecture Notes in Computer Science , 1380 , 1 , 10

Palabras clave: polinomios sobre cuerpos finitos; tests de irreducibilidad
Areas del 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 / criptografia
Medio de divulgación: Papel;

http://www.informatik.uni-trier.de/~ley/db/conf/latin/latin98.html

Completo

VIOLA, A.; POBLETE, P

Analysis of linear probing hashing with buckets , 1996

Evento: Internacional , 4th European Symposium on Algorithms , 1996

Anales/Proceedings: Lecture Notes in Computer Science , 1136 , 221 , 233

Palabras clave: linear probing hashing with buckets
Areas del conocimiento: Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / analisis de algoritmos
Medio de divulgación: Papel; *Idioma/Pais:* Inglés/Estados Unidos;

http://www.informatik.uni-trier.de/~ley/db/conf/esa/esa96.html

Completo

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

Analysis of a Hashing Scheme by a New Transform , 1994

Evento: Internacional , 2nd European Symposium on Algorithms , 1994

Anales/Proceedings: Lecture Notes in Computer Science , 855 , 94 , 105

Palabras clave: linear probing hashing; Transformada Diagonal de Poisson
Areas del conocimiento: Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / analisis de algoritmos
Medio de divulgación: Papel;

Completo

VIOLA, A.; LI, M

Learning Secondary Structure of Proteins , 1994

Evento: Internacional , 6th International Conference on Computing and Information , 1994

Palabras clave: estructura secundaria de proteinas
Areas del conocimiento: Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / bioinformática
Medio de divulgación: Papel;

Producción técnica

Trabajos Técnicos

Asesoramiento

VIOLA, A.
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) , Colaborar en la propuesta de restructura de dicha CV y su viabilidad futura , 2005 , 36

Institución financiadora: Sin fines de lucro

Palabras clave: TICs y desarrollo social; Sociedad de la Información
Areas del 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; *Disponibilidad:* Restricta; *Ciudad:* /República Dominicana

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 PImienta, 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 metasitio 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 restructura, refinanciamiento y relanzamiento, y más específicamente estamos pensando en crear una CVA (Comunidad Virtual de Aprendizaje) basado en el contenido actualizado de dicho metasitio. 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.

Consultoría

VIOLA, A.
Tecnologías de la Información aplicadas a la Salud , Asesor de la red Eurolatis para presentar proyectos en los programas marco de la Unión Europea , 2001 , 6

Institución financiadora: Unión Europea

Palabras clave: TICs y desarrollo social; TICs y su uso en salud; Sociedad de la Información
Areas del 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; *Disponibilidad:* Restricta; *Ciudad:* La Habana/Cuba

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 Uruugay. 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 evaluacion, 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.

Consultoría

VIOLA, A.

Tecnologías de la Información aplicadas a la Educación , Asesor de la red Eurolatis para presentar proyectos en los programas marco de la Unión Europea , 2000 , 6

Institución financiadora: Unión Europea

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

Areas del 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; *Disponibilidad:* Restricta; *Ciudad:* Santiago de Chile - Montevideo/Chile

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 Uruugay. 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 evaluacion, 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.

Consultoría

VIOLA, A.

Miembro del Steering Committee de Eurolatis , Eurolatis era una red Union Europea - América Latina y Caribe, para el desarrollo de la Sociedad de la Información en la región , 1999 , 36

Institución financiadora: Unión Europea

Palabras clave: TICs y desarrollo social; Sociedad de la Información

Areas del conocimiento: Ingeniería y Tecnología / Ingeniería Eléctrica, Ingeniería Electrónica e Ingeniería de la Información / Ingeniería de Sistemas y Comunicaciones / Tecnologías de la Comunicación en Información

Disponibilidad: Restricta; *Ciudad:* /Uruguay

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 Uruugay. 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.

Otros

Cursos de corta duración dictados

Perfeccionamiento

Análisis de algoritmos , 2002

Argentina , Español , Papel

Tipo de participación: Docente, *Unidad:* Escuela de Ciencias de la Computación (ECI), *Duración:* 1 semanas

Universidad de Buenos Aires , Buenos Aires

Institución Promotora/Financiadora: Universidad de Buenos Aires

Palabras clave: Análisis de Algoritmos

Areas del conocimiento: Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / analisis de algoritmos - Combinatoria

Edición o revisión

Anales

Proceedings LATIN 2014 , 2014

Uruguay , Inglés

Número de páginas: 700,

Areas del conocimiento: Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Teoría de la Computación

Edición o revisión

Anales

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

Uruguay , Inglés , 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 del conocimiento: Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Teoría de la Computación

Edición o revisión

Revista

Selected papers from LATIN 2000 , 2003

Uruguay , Inglés , Papel

Número de páginas: 350, *Editorial:* Elsevier,

Amsterdam

Institución Promotora/Financiadora: Theoretical Computer Science (TCS)

Palabras clave: Teoría de la Computación

Areas del conocimiento: Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Teoría de la Computación

Edición o revisión

Revista

Selected papers from CLEI 2002 , 2003

Uruguay , Inglés , Internet , http://www.clei.cl/cleiej/

Número de páginas: 120, *Editorial:* CLEI,

Chile

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

Palabras clave: Informática

Areas del 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.

Organización de eventos

Concierto

ITW Information Theory Workshop , 2006

Uruguay , Inglés , CD-Rom , http://www.fing.edu.uy/itw06

Duración: 1 semanas

Evento itinerante: SI, *Catálogo:* SI

Maldonado , Punta del Este

Institución Promotora/Financiadora: Facultad de Ingeniería

Palabras clave: Teoría de la Información

Areas del 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 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.

Organización de eventos

Congreso

LATIN 2000 , 2000

Uruguay , Inglés , http://www.fing.edu.uy/inco/eventos/latin-2000

Duración: 1 semanas

Evento itinerante: SI, *Catálogo:* SI

Maldonado , Punta del Este

Institución Promotora/Financiadora: Instituto de Computación

Palabras clave: Teoría de la Computación

Areas del 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.

Organización de eventos

Congreso / Organización

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

Canadá , Inglés , Internet , http://www.fields.utoronto.ca/programs/scientific/13-14/efficient/

Duración: 1 semanas

Evento itinerante: NO, *Catálogo:* NO

CANADÁ , Waterloo, Ontario

Palabras clave: Space Efficient Data Structures

Areas del conocimiento: Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Teoría de la Computación

Organización de eventos

Otro

Formal Methods in Security , 2007

Uruguay , Español , Internet

Duración: 1 semanas

Evento itinerante: SI, *Catálogo:* NO

Montevideo , Montevideo

Institución Promotora/Financiadora: STIC-AMSUD

Palabras clave: Information Security

Areas del 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

Otra producción técnica

TUBA NUMBERS , 2007

Estados Unidos , Inglés , Internet , 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

Areas del conocimiento: Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / analisis 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).

Otra producción técnica

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

Uruguay , Inglés , Papel

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

Holanda , Amsterdam

Institución Promotora/Financiadora: European Association of Theoretical Computer Science

Palabras clave: Teoría de la Computación

Areas del 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

2009 / 2010

Institución financiadora: Presidente de concurso de tesis de Maestría CLEI - UNESCO

Cantidad: Mas de 20

Presidente de concurso de tesis de Maestría CLEI - UNESCO , Uruguay

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

Evaluación de Proyectos

2008 / 2008

Institución financiadora: Universidad de San Luis

Cantidad: Menos de 5

Universidad de San Luis , Argentina

Evaluador externo de la propuesta de tesis de doctorado de Nora Reyes.

Evaluación de Proyectos

2006 / 2008

Institución financiadora: PDT - ANII

Cantidad: Mas de 20

PDT - ANII , Uruguay

Pertenencia a Comisión Técnica Asesora en el área de Ciencias Básicas en llamados PDT y fondos Clemente Estable.

Evaluación de Proyectos

2005 / 2008

Institución financiadora: Conicet

Cantidad: De 5 a 20

Conicet , Argentina

Evaluador perióidco de varios proyectos de investigación financiados por dicha institución desde 2005.

Evaluación de Proyectos

2005 / 2008

Institución financiadora: cooperación internacional México - Argentina

Cantidad: Menos de 5

cooperación internacional México - Argentina , Argentina

Evaluación de dos proyectos de cooparación internacional entre Argentina y México solicitado por la contraparte Argentina.

Evaluación de Proyectos

2004 / 2008

Institución financiadora: ECOS - cooperación Argentina - Francia

Cantidad: Menos de 5

ECOS - cooperación Argentina - Francia , Francia

Evaludador de dos propuestas de proyectos ECOS entre grupos de investigación en Argentina y en Francia.

Evaluación de Proyectos

1996 / 2008

Institución financiadora: CLEI - UNESCO

Cantidad: Mas de 20

CLEI - UNESCO , Uruguay

Desde 1996 he participado en varios tribunales del concurso Latinoamericano de Tesis de Maestría en Informática financiado conjuntamente por el CLEI (Centro Latinoamericando 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 Latinoaméricana de Informática.

Evaluación de Eventos

2014

Nombre: ALEA 2015 (co-organizador),

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

Evaluación de Eventos

2014

Nombre: LATINCRYPT 2014,

Evaluación de Eventos

2014

Nombre: Co-organizador de la escuela “Combinatoria Analítica y Dinámica. Aplicaciones”,

UNGS

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

Evaluación de Eventos

2014

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

Evaluación de Eventos

2014

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

Evaluación de Eventos

2013

Nombre: LATIN 2014 (presidente del comité de programa),

Uruguay

Evaluación de Eventos

2013

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

Canadá

Evaluación de Eventos

2013

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

Canadá

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

Evaluación de Eventos

2013

Nombre: Co-organizador de escuela de criptografía ASCrypto 2013,

Capes

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

Evaluación de Eventos

2012

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

India

Evaluación de Eventos

2011

Nombre: LATIN 2012,

Perú

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

Evaluación de Eventos

2011

Nombre: LATINCRYPT 2012,

Chile

Evaluación de Eventos

2011

Nombre: Co-organizador de escuela de criptografía ASCrypto 2011,

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.

Evaluación de Eventos

2010

Nombre: LATINCRYPT 2010,

México

Miembro del Steering Committee de LATINCRYPT que creò esta conferencia. Es la versiòn latinoamericana de la prestigiosa conferencia CRYPTO

Evaluación de Eventos

2010

Nombre: Second International Conference on Emergin Applications of Information Technology (EAIT 2011),

India

Conference Proceedings publicados por la IEEE Computer Society Conference Publishing Services

Evaluación de Eventos

2009

Nombre: LATIN 2010 (Latin American Theoretical INformatics) ,

México

Miembro del Comité de Programa

Evaluación de Eventos

2009

Nombre: V Congreso Iberoamericano de Seguridad Informática (CIBSI09),

Uruguay

Miembro del Comité de Programa

Evaluación de Eventos

2009

Nombre: Sistema nacional de investigador,

Uruguay

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

Evaluación de Eventos

2008

Nombre: ANALCO 2008 (Analytic Algorithms and Combinatorics),

Estados Unidos

Miembro de Comité de Programa Organizado por la SIAM

Evaluación de Eventos

2008

Nombre: LATIN 2008 (Latin American Theoretical INformatics),

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.

Evaluación de Eventos

2008

Nombre: LAGOS/GRACO 2009,

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.

Evaluación de Eventos

2008

Nombre: Sistema Nacional de Investigador,

Uruguay

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

Evaluación de Eventos

2007

Nombre: CLEI 2007 (Conferencia Latinoamericana de Informática),

Costa Rica

Miembro de Comité de Programa

Evaluación de Eventos

2007

Nombre: II Conference on Analysis of Algorithms (AofA7),

Francia

Miembro de Comité de Programa

Evaluación de Eventos

2007

Nombre: IV Congreso Iberoamericano de Seguridad Informática (CIBSI07),

Argentina

Miembro de Comité de Programa

Evaluación de Eventos

2006

Nombre: IFIP International Conference on Theoretical Computer Science (IFIP TCS 2006),

Chile

Miembro de Comité de Programa

Evaluación de Eventos

2006

Nombre: LATIN 2006,

Chile

Miembro de Comité de Programa

Evaluación de Eventos

2006

Nombre: IEEE Information Theory Workshop (ITW06),

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.

Evaluación de Eventos

2005

Nombre: III Congreso Iberoamericano de Seguridad Informática (CIBSI 05),

Chile

Miembro de Comité de Programa

Evaluación de Eventos

2005

Nombre: IFIP/ACM Latin American Networking Conference (LANC05),

Colombia

Miembro de Comité de Programa

Evaluación de Eventos

2005

Nombre: Encuentro Internacional de Ciencias de la Computación (ENC 2005),

México

Miembro de Comité de Programa

Evaluación de Eventos

2005

Nombre: I International Conference on the Analysis of Algorithms (AofA05),

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.

Evaluación de Eventos

2004

Nombre: Encuentro Internacional de Ciencias de la Computación (ENC 2004),

México

Miembro del Comité de Programa

Evaluación de Eventos

2003

Nombre: CLEI 2003 (Conferencia Latinoamericana de Informatica),

Bolivia

Miembro del Comité de Programa

Evaluación de Eventos

2003

Nombre: IFIP/ACM Latin American Networking Conference (LANC03),

Bolivia

Miembro del Comité de Programa

Evaluación de Eventos

2003

Nombre: WAIT 2003 (Workshop Argentino de Informática Teórica),

Argentina

Miembro del Comité de Programa

Evaluación de Eventos

2002

Nombre: CLEI 2002 (Conferencia Latinoamericana de Informatica),

Uruguay

Presidente del Comité de Programa

Evaluación de Eventos

2002

Nombre: IFIP International Conference on Theoretical Computer Science (IFIP TCS 2002),

Canadá

Miembro del Comité de Programa

Evaluación de Eventos

2001

Nombre: ACM - SIGCOMM Conferencia sobre Comunicación de Datos en Latinoamérica y el Caribe,

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.

Evaluación de Eventos

2000

Nombre: LATIN 2000 (Latin American Theoretical INformatics),

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.

Evaluación de Eventos

1997

Nombre: WAIT 1997 (Workshop Argentino de Informática Teórica),

Argentina

Miembro del Comité de Programa

Evaluación de Publicaciones
2009 / 2013
Nombre: ACM Transactions on Algorithms,
Cantidad: Menos de 5

Evaluación de Publicaciones
2008 / 2013
Nombre: Combinatorics, Probability and Computing,
Cantidad: Menos de 5
Nueva revista online de Cambridge University Press

Evaluación de Publicaciones
2005 / 2010
Nombre: RAIRO,
Cantidad: Menos de 5
Revista francesa de informática teórica

Evaluación de Publicaciones
2002 / 2013

Nombre: IEEE Transactions on Information Theory,
Cantidad: Mas de 20
Es la revista más importante del mundo en Teoría de la Información

Evaluación de Publicaciones
1998 / 2013
Nombre: Random Structures and Algorithms,
Cantidad: Menos de 5
Es la revista más prestigiosa en Random Structures

Evaluación de Publicaciones
1998 / 2010
Nombre: Algorithmica,
Cantidad: Menos de 5
Una de las revistas más prestigiosas en algoritmos

Evaluación de Publicaciones
1996 / 2013
Nombre: Theoretical Computer Science,
Cantidad: De 5 a 20
Es una de las revistas más prestigiosas en Teoría de la Computación

Evaluación de Premios

2010 / 2010
Nombre: Premios Anuales de Literatura,
Cantidad: Menos de 5
Ministerio de Educación y Cultura , Uruguay
categoría: OBRAS SOBRE INVESTIGACIÓN Y DIFUSIÓN CIENTÍFICA.

Evaluación de Convocatorias Concursables
2010 / 2011
Nombre: Acreditación de Carreras Universitarias de Computación en Argentina,
Cantidad: De 5 a 20
CONEAU , Argentina
Evaluador extranjero en el proceso de acreditación de carreras de Computación en Argentina.

Evaluación de Convocatorias Concursables

2010 / 2013

Nombre: ANII - diferentes convocatorias,

Cantidad: Mas de 20

ANII

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

Evaluación de Convocatorias Concursables

2009

Nombre: Proyectos de Iniciación a la Investigación Científica,

Cantidad: De 5 a 20

CSIC - UDELAR , Uruguay

Participación en la comisión de evaluación

Evaluación de Convocatorias Concursables

2008

Nombre: FCE,

Cantidad: De 5 a 20

ANII , Uruguay

Integrante de la comisiòn técnica del área básica

Evaluación de Convocatorias Concursables

2006

Nombre: PDT,

Cantidad: De 5 a 20

Ministerio de Educación y Cultura , Uruguay

Integrante de comisión Técnica del área básica

Formación de RRHH

Tutorías concluidas

Posgrado

Tesis de maestría

Combinatoria Analítica y Aplicaciones , 2014

Tipo de orientación: Tutor único o principal

Nombre del orientado: Pablo Rotondo

Programa de Desarrollo de las Ciencias Básicas , Uruguay , Maestría en Informática

Palabras clave: Combinatoria Analítica

Areas del conocimiento: Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / combinatoria analítica

Pais/Idioma: Uruguay/Español

Tesis de doctorado

Tree models: Algorithms and Information Theoretic Properties , 2009

Tipo de orientación: Cotutor o Asesor

Nombre del orientado: Alvaro Martin

Facultad de Ingeniería - UDeLaR , Uruguay , Doctorado en Informática (UDELAR-PEDECIBA)

Palabras clave: Type classes; Tree Models

Areas del conocimiento: Ingeniería y Tecnología / Ingeniería Eléctrica, Ingeniería Electrónica e Ingeniería de la Información / Telecomunicaciones / Teoria de la Información

Pais/Idioma: Uruguay/Inglés

Información adicional: El orientador de Tesis fue el Dr. Gadiel Seroussi.

Tesis de maestría

Análisis del algoritmo de compresión PPM , 2006

Tipo de orientación: Cotutor o Asesor

Nombre del orientado: Jorge Merlino

Facultad de Ingeniería - UDeLaR , Uruguay , Maestría en Informática (UDELAR-PEDECIBA)

Palabras clave: Algoritmo PPM
Areas del conocimiento: Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Teoría de la Información
Medio de divulgación: Papel, *Pais/Idioma:* Uruguay/Español

Información adicional: Supervisor de esutdios y co-orientador de tesis junto con Marcelo Weinberger (HP Labs, California)

Tesis de maestría

Texture Mixing via Universal Simulation , 2005

Tipo de orientación: Cotutor o Asesor

Nombre del orientado: Gustavo Brown

Facultad de Ingeniería - UDeLaR , Uruguay , Maestría en Informática (UDELAR-PEDECIBA)

Palabras clave: simulación de texturas; Algoritmo de Lempel-Ziv
Areas del conocimiento: Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Teoría de la Información

Medio de divulgación: Papel, *Pais/Idioma:* Uruguay/Inglés
Información adicional: Orientación de Tesis de parte de Gadiel Seroussi (HP Labs, California) y Guillermo Sapiro (U. de Minnesota)

Tesis de maestría

Implementacion eficiente de modelos de markov dispersos usando algoritmos genéticos , 2005

Tipo de orientación: Cotutor o Asesor

Nombre del orientado: Alix Lhéritier

Facultad de Ingeniería - UDeLaR , Uruguay , Maestría en Informática (UDELAR-PEDECIBA)

Palabras clave: Modelos de Markov dispersos
Areas del conocimiento: Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Teoría de la Información
Medio de divulgación: Papel, *Pais/Idioma:* Uruguay/Español

Información adicional: Supervisor de estudios y co-orientador de tesis junto con Gadiel Seroussi (HP Labs, california)

Grado

Tesis/Monografía de grado

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

Tipo de orientación: Tutor único o principal

Nombre del orientado: Sebastián Fonseca / María Cecilia García

Facultad de Ingeniería - UDeLaR , Uruguay , Ingeniería en Computación
Areas del conocimiento: Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / criptografia

Pais/Idioma: Uruguay/Español

Tesis/Monografía de grado

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

Nombre del orientado: Adrian Silveira

Facultad de Ingeniería - UDeLaR , Uruguay , Ingeniería en Computación

Palabras clave: Firma Digital; Asistente de Pruebas; Métodos Formales
Areas del conocimiento: Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / criptografia
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Métodos Formales
Pais/Idioma: Uruguay/Español

Información adicional: Co-dirección con Gustavo Betarte en colaboración con Gilles Barthes (España).

Tesis/Monografía de grado

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

Nombre del orientado: Cecilia Parodi y Gaston Simone

Facultad de Ingeniería - UDeLaR , Uruguay , Ingeniería en Computación

Palabras clave: Códigos Reed - Solomon; Decodificación por Listas
Areas del conocimiento: Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Teoría de Códigos
Medio de divulgación: Papel, *Pais/Idioma:* Uruguay/Español
Información adicional: Proyecto co-tutoreado por Fernando fernández y con la participación y proyesta de proyecto de Gadiel Seroussi (HP Labs, California)

Tesis/Monografía de grado

Generaciòn aleatoria eficiente de funciones booleanas resilientes , 2009

Tipo de orientación: Tutor único o principal

Nombre del orientado: Nicolàs Carrasco

Facultad de Ingeniería - UDeLaR , Uruguay , Ingeniería en Computación

Palabras clave: funciones booleanas resilientes
Areas del conocimiento: Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Funciones booleanas, criptografía
Pais/Idioma: Uruguay/Español

Información adicional: En colaboraciòn con Jean-Marie Le Bars de la Universidad de Caen.

Tesis/Monografía de grado

Predicción de Estructura Secundaria de Proteínas , 2006

Nombre del orientado: Elisa Budelli

Facultad de Ingeniería - UDeLaR , Uruguay , Ingeniería en Computación

Palabras clave: prediccion de estructura secundaria de proteinas
Areas del conocimiento: Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / bioinformática
Medio de divulgación: Papel, *Pais/Idioma:* Uruguay/Español

Información adicional: Trabajo co-dirigido con Fernando Alvarez de la Facultad de Ciencias

Tesis/Monografía de grado

Algoritmos óptimos de compresión , 2004

Nombre del orientado: Florencia da Silveira: Karina Alvarez

Facultad de Ingeniería - UDeLaR , Uruguay , Ingeniería en Computación

Palabras clave: Algoritmo Context
Areas del conocimiento: Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Teoría de la Información
Pais/Idioma: Uruguay/Español

Información adicional: Co-dirigido con Alvaro Martín

Tesis/Monografía de grado

Corrección de errores para distribución de datos en redes , 2004

Nombre del orientado: Fernando Fernández

Facultad de Ingeniería - UDeLaR , Uruguay , Ingeniería en Computación

Palabras clave: Codigos correctores de errores
Areas del 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
Medio de divulgación: Papel, *Pais/Idioma:* Uruguay/Español

Tesis/Monografía de grado

Codigos de paridad de baja densidad , 2003

Nombre del orientado: Alix Lhéritier

Facultad de Ingeniería - UDeLaR , Uruguay , Ingeniería en Computación

Palabras clave: Codigos LDPC
Areas del conocimiento: Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Teoría de Códigos
Medio de divulgación: Papel, *Pais/Idioma:* Uruguay/Español

Tesis/Monografía de grado

El comercio electrónico y los sistemas de pago online , 2003

Nombre del orientado: César Ponce: José Pedro Rabinovich

Facultad de Ingeniería - UDeLaR , Uruguay , Ingeniería en Computación

Palabras clave: pagos online
Areas del conocimiento: Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / criptografia
Medio de divulgación: Papel, *Pais/Idioma:* Uruguay/Español

Tesis/Monografía de grado

Simulación de un mercado de transacciones financieras por internet , 2002

Nombre del orientado: Luján Camino; Marcos Viera; Diego Borghi; Elisa Bittencourt

Facultad de Ingeniería - UDeLaR , Uruguay , Ingeniería en Computación

Palabras clave: pagos online
Areas del conocimiento: Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / criptografia
Medio de divulgación: Papel, *Pais/Idioma:* Uruguay/Español

Tesis/Monografía de grado

Inserción de marcas de tiempo en certificados digitales , 2002

Nombre del orientado: Ricardo Martínez

Facultad de Ingeniería - UDeLaR , Uruguay , Ingeniería en Computación

Palabras clave: marcas de tiempo
Areas del conocimiento: Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / criptografia
Medio de divulgación: Papel, *Pais/Idioma:* Uruguay/Español
Información adicional: En coordinación con la autoridad certificadora del correo uruguayo.

Tesis/Monografía de grado

Criptografía para dispositivos de bajos recursos , 2001

Nombre del orientado: Santiago Jaureche; Jorge Merlino

Facultad de Ingeniería - UDeLaR , Uruguay , Ingeniería en Computación

Palabras clave: dispositivos de bajos recursos
Areas del conocimiento: Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / criptografia
Medio de divulgación: Papel, *Pais/Idioma:* Uruguay/Español

Tesis/Monografía de grado

Estudio de Transacciones electrónicas en internet , 2001

Nombre del orientado: Daniel Brignardello

Facultad de Ingeniería - UDeLaR , Uruguay , Ingeniería en Computación

Palabras clave: transacciones electrónicas por internet
Areas del conocimiento: Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / criptografia
Medio de divulgación: Papel, *Pais/Idioma:* Uruguay/Español

Tesis/Monografía de grado

Relevamiento de escenarios y técnicas para realización de proyectos de comercio electrónico , 2000

Nombre del orientado: Leonardo Dominguez; Cecilia Fernández

Facultad de Ingeniería - UDeLaR , Uruguay , Ingeniería en Computación

Palabras clave: comercio electrónico
Areas del conocimiento: Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / criptografia
Medio de divulgación: Papel, *Pais/Idioma:* Uruguay/Español

Tesis/Monografía de grado

Sistema de comercio electrónico , 1999

Nombre del orientado: Pablo Torres

Facultad de Ingeniería - UDeLaR , Uruguay , Ingeniería en Computación

Palabras clave: comercio electrónico
Areas del conocimiento: Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / criptografia
Pais/Idioma: Uruguay/Español

Tesis/Monografía de grado

Inserción de marcas de agua en imágenes digitales , 1999

Nombre del orientado: Fabian Martínez; Gabriela Delfino

Facultad de Ingeniería - UDeLaR , Uruguay , Ingeniería en Computación

Palabras clave: watermarking
Areas del conocimiento: Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / criptografia
Pais/Idioma: Uruguay/Español

Tesis/Monografía de grado

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

Nombre del orientado: J. P. Fernández: Uruguay Larre Borges; Francisco Pereira

Facultad de Ingeniería - UDeLaR , Uruguay , Ingeniería en Computación

Palabras clave: recuperación de información
Areas del conocimiento: Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Sistemas de Información
Medio de divulgación: Papel, *Pais/Idioma:* Uruguay/Español

Tesis/Monografía de grado

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

Nombre del orientado: Federico Molfino; P.ablo Sartor: Fernando Vignali

Facultad de Ingeniería - UDeLaR , Uruguay , Ingeniería en Computación

Palabras clave: recuperación de información
Areas del conocimiento: Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Sistemas de Información

Pais/Idioma: Uruguay/Español

Tesis/Monografía de grado

Buscador Académico Uruguayo , 1997

Nombre del orientado: Alfredo Espasandin; Ricardo Martínez

Facultad de Ingeniería - UDeLaR , Uruguay , Ingeniería en Computación

Palabras clave: recuperación de información
Areas del conocimiento: Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Sistemas de Información
Medio de divulgación: Papel, *Pais/Idioma:* Uruguay/Español

Tutorías en marcha

Posgrado

Tesis de doctorado

An ́alisis Dinámico en Combinatoria de Palabras , 2015

Tipo de orientación: Cotutor en pie de igualdad

Nombre del orientado: Pablo Rotondo

Facultad de Ingeniería - UDeLaR , Uruguay , Doctorado en Informática (UDELAR-PEDECIBA)

Palabras clave: Análisis dinámico de algoritmos

Areas del conocimiento: Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación

Pais/Idioma: Francia/Inglés

Información adicional: 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.

Tesis de maestría

Seguridad en redes GSM , 2011

Tipo de orientación: Cotutor o Asesor

Nombre del orientado: Eduardo Cota

Facultad de Ingeniería - UDeLaR , Uruguay , Maestría en Ingeniería (Ingeniería Eléctrica)

Palabras clave: Redes GSM; Seguridad

Areas del conocimiento: Ingeniería y Tecnología / Ingeniería Eléctrica, Ingeniería Electrónica e Ingeniería de la Información / Telecomunicaciones / Seguridad en Redes GSM

Pais/Idioma: Uruguay/Español

Información adicional: Co-dirección de tesis junto con Eduardo Giménez. El supervisor de estudios es Pablo Belzarena.

Grado

Tesis/Monografía de grado

Funciones Booleanas inmunes a la correlación y ataques a AES en tarjetas inteligentes , 2016

Tipo de orientación: Tutor único o principal

Nombre del orientado: Francisco Castro

Facultad de Ingeniería - UDeLaR , Uruguay , Licenciatura en Computación

Palabras clave: ataque AES

Areas del 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 / criptografia

Pais/Idioma: Uruguay/Español

Otros datos relevantes

Premios y títulos

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

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

1987 BECA PEDECIBA para realizar posgrado en Canadá Pedeciba

1990 International Student Fee Waiver Universidad de Waterloo

1989 Student Fellowship NSERC - Canadá

2009 Sistema Nacional de Investigador (Nivel II) ANII

1997 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. http://www-cs-faculty.Stanford.EDU/~knuth/

2009 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. http://algo.inria.fr/flajolet/Publications/books.html

2003 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. http://math-www.uni-paderborn.de/mca/

2001 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. Wiley-Interscience

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

2004 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. Capman & Hall/CRC

1998 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 CRC-PRESS

2001 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. AofA

2007 Autor de la secuencia TUBA NUMBERS (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 investigacion 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)

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

Jurado/Integrante de comisiones evaluadoras de trabajos académicos

Tesis

Candidato: Agustín Mullin

CALEGARI, D.; VARGAS, G.; VIOLA, A.

Metadata-based Provenance , 2015

Tesis (Maestría en Informática (UDELAR-PEDECIBA)) - Facultad de Ingeniería - UDeLaR - Uruguay

Referencias adicionales: Uruguay , Inglés

Palabras clave: metadatos; provenance

Areas del conocimiento: Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Sistemas de Información

Tesis

Candidato: Daniel Perovich

VIOLA, A.

2008

Tesis (Maestría en Informática (UDELAR-PEDECIBA)) - Facultad de Ingeniería - UDeLaR - Uruguay

Referencias adicionales: Uruguay , Español

Tesis

Candidato: Javier Preciozzi

VIOLA, A.

2005

Tesis (Maestría en Informática (UDELAR-PEDECIBA)) - Facultad de Ingeniería - UDeLaR - Uruguay

Referencias adicionales: Uruguay , Español

Tesis

Candidato: Silvia Viola

VIOLA, A.

2004

Tesis (Maestría en Física (UDELAR-PEDECIBA)) - Facultad de Ciencias - UDeLaR - Uruguay

Referencias adicionales: Uruguay , Español

Tesis

Candidato: Gabriele Facciolo

VIOLA, A.

2004

Tesis (Maestría en Informática (UDELAR-PEDECIBA)) - Facultad de Ingeniería - UDeLaR - Uruguay

Referencias adicionales: Uruguay , Español

Tesis

Candidato: Leslie Murray

VIOLA, A.

2003

Tesis (Maestría en Informática (UDELAR-PEDECIBA)) - Facultad de Ingeniería - UDeLaR - Uruguay

Referencias adicionales: Uruguay , Español

Tesis

Candidato: Antonio Vera

B. VALLÉE; FLAJOLET P.; HANROT G.; MAAS A.; VIOLA, A.; BERTHÈ V.; DAUDÈ H.

Analyses de l algorithme de Gauss. Applications a l analyse de l algorithme LLL , 2009

Tesis (Doctorat Specialite: Informatique) - Universite de Caen - Francia

Referencias adicionales: Francia , Francés

Palabras clave: Algoritmo LLL

Areas del conocimiento: Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / analisis de algoritmos

Otros tipos

Candidato: Varios Candidatos

GORDILLO, S; MATAMALA, M; VIOLA, A.

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

Otra participación (Ingeniería) - Universidad de Buenos Aires - Argentina

Referencias adicionales: Argentina , Español

Palabras clave: Profesor Regular Asociado

Areas del conocimiento: Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Estructuras de Datos y Algoritmos

Otros tipos

Candidato: Varios Candidatos

GORDILLO, S; JOFRE, A; VIOLA, A.

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

Otra participación (Ingeniería) - Universidad de Buenos Aires - Argentina

Referencias adicionales: Argentina , Español

Palabras clave: Profesor Regular Asociado

Areas del conocimiento: Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Ingeniería de Software

Presentaciones en eventos

Seminario

Distributional analisis of the parking problem and the Robin Hood Linear probing algorithm with buckets , 2010

Tipo de participación: Expositor oral,

Referencias adicionales: Francia; *Nombre del evento:* Invitacion a participar en el seminario del laboratorio; *Nombre de la institución promotora:* Ecole Polytechnique

Palabras clave: hashing; parking problem with buckets; linear probing with buckets; Tuba Numbers

Areas del conocimiento: Ciencias Naturales y Exactas / Matemáticas / Matemática Aplicada / Analisis de algorithmos y combinatoria

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

Seminario

Efficient Data Structures for Universal Denoising , 2008

Tipo de participación: Expositor, *Carga horaria:* 30

Referencias adicionales: Alemania; *Nombre del evento:* Dagstuhl Seminar on Data Structures; *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 presentaciónes 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 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.

Seminario

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

Tipo de participación: Expositor,

Referencias adicionales: Bélgica; *Nombre del evento:* 11th seminar on Analysis of Algorithms; *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.

Seminario

Adaptive Sampling Strategies for Quickselect , 2004

Tipo de participación: Expositor,

Referencias adicionales: Estados Unidos; *Nombre del evento:* 10th Seminar on Analysis of Algorithms; *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.

Seminario

On worst case Robin Hood Hashing , 2003

Tipo de participación: Expositor,

Referencias adicionales: Italia; *Nombre del evento:* 9th Seminar on Analysis of Algorithms; *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.

Seminario

Exact distribution of individual displacements in linear probing hashing , 2002

Tipo de participación: Expositor,

Referencias adicionales: Austria; *Nombre del evento:* 8th Seminar on Analysis of Algorithms; *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.

Seminario

Analysis of Rabin`s Irreducibility Test for Polynomials over Finite Fields , 2001

Tipo de participación: Conferencista Invitado,

Referencias adicionales: Francia; *Nombre del evento:* 7th Seminar on Analysis of Algorithms; *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.

Seminario

Open problems related with Linear Probing Hashing with Buckets , 2000

Tipo de participación: Expositor,

Referencias adicionales: Polonia; *Nombre del evento:* 6th Seminar on Analysis of Algorithms; *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.

Seminario

The Effect of Deletions on Different Insertion Disciplines for Hash Tables , 1999

Tipo de participación: Expositor,

Referencias adicionales: España; *Nombre del evento:* 5th Seminar on Analysis of Algorithms; *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.

Seminario

Analysis of the total displacement in a linear probing hash table. , 1997

Tipo de participación: Expositor,

Referencias adicionales: Alemania; *Nombre del evento:* Dagstuhl Seminar on Data Structures; *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 presentaciónes 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.

Seminario

The analysis of linear probing hashing with buckets , 1997

Tipo de participación: Expositor,

Referencias adicionales: Estados Unidos; *Nombre del evento:* DIMACS Seminar on Probabilistic Analysis of Algorithms; *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.

Seminario

The diagonal Poisson transform and its application to the analysis of a hashing scheme , 1995

Tipo de participación: Expositor,

Referencias adicionales: Alemania; *Nombre del evento:* Dagstuhl Seminar on Analysis of Algorithms; *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 presentaciónes 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.

Simposio

Philippe Flajolet and his theoretical contributions in the analysis of hashing algorithms , 2011

Tipo de participación: Conferencista Invitado,

Referencias adicionales: Francia; *Nombre del evento:* Philippe Flajolet and Analytic Combinatorics; *Nombre de la institución promotora:* INRIA

Palabras clave: Hashing Algorithms

Areas del 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.

Simposio

Boolean Functions in cryptography , 2011

Tipo de participación: Conferencista Invitado,

Referencias adicionales: Brasil; *Nombre del evento:* Escuela de Criptografia SP-ASCrypto; *Nombre de la institución promotora:* CNPQ

Palabras clave: funciones booleanas

Areas del conocimiento: Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / criptografia

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.

Simposio

Some asyptotic issues related with the exact distribution of Individual Displacements in Linear Probing Hashing , 2009

Referencias adicionales: Canadá;

Palabras clave: linear probing hashing

Areas del conocimiento: Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / analisis de algoritmos

Simposio

Combinatorial characterization of Resilient Functions , 2007

Tipo de participación: Expositor,

Referencias adicionales: Estados Unidos; *Nombre del evento:* Workshop on Information Theory and Applications; *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.

Simposio

Adaptive Sampling Strategies for Quickselect , 2003

Tipo de participación: Conferencista Invitado,

Referencias adicionales: Brasil; *Nombre del evento:* Workshop on Combinatorics, Algorithms and Applications; *Nombre de la institución promotora:* Universidad de San Pablo

Simposio

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

Tipo de participación: Conferencista Invitado,

Referencias adicionales: Canadá; *Nombre del evento:* Montreal - Ottawa Analysis of Algorithms Workshop; *Nombre de la institución promotora:* Universidad de Carleton

Encuentro

INFORMATION TECHNOLOGIES TO THE HELP OF CITIZEN PARTICIPATION IN PUBLIC DECISIONS AND PUBLIC EDUCATION , 2008

Tipo de participación: Expositor,

Referencias adicionales: Argentina; *Nombre del evento:* Grand Challenges in Computer Science Research in Latin America Workshop; *Nombre de la institución promotora:* CLEI y SBC (Sociedad Brasilera de Computación)

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

Areas del 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.

Encuentro

KnuthFest , 2002

Tipo de participación: Otros,

Referencias adicionales: Estados Unidos; *Nombre del evento:* KnuthFest; *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 partiparon 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'.

Encuentro

The symbolic method in combinatorics , 2000

Tipo de participación: Conferencista Invitado,

Referencias adicionales: Brasil; *Nombre del evento:* Encuentro Brasilero de Combinatoria; *Nombre de la institución promotora:* Universidad de San Pablo

Indicadores de producción

Producción bibliográfica	*41*
Artículos publicados en revistas científicas	*17*
Completo (Arbitrada)	17
Artículos aceptados para publicación en revistas científicas	*0*

Trabajos en eventos	*19*
Completo (No Arbitrada)	11
Resumen expandido (Arbitrada)	6
Resumen expandido (No Arbitrada)	2
Libros y capítulos de libros publicados	*5*
Capítulo de libro publicado	1
Libro compilado	4
Textos en periódicos	*0*
Documentos de trabajo	*0*
Producción técnica	*15*
Productos tecnológicos	*0*
Procesos o técnicas	*0*
Trabajos técnicos	*4*
Otros tipos	*11*
Evaluaciones	*61*
Evaluación de Proyectos	7
Evaluación de Eventos	41
Evaluación de Publicaciones	7
Evaluación de Premios	1
Evaluación de Convocatorias Concursables	5
Formación de RRHH	*27*
Tutorías/Orientaciones/Supervisiones concluidas	*24*
Tesis de maestría	4
Tesis de doctorado	1
Tesis/Monografía de grado	19
Tutorías/Orientaciones/Supervisiones en marcha	*3*
Tesis de maestría	1
Tesis de doctorado	1
Tesis/Monografía de grado	1

Sistema Nacional de Investigadores