ALFREDO VIOLA DEAMBROSIS

Dr

viola@fing.edu.uy
Magallanes 910, Montevideo URUGUAY. CP 11200
24102415

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

Fecha de publicación: 28/12/2023
Última actualización: 22/12/2023

Datos Generales

DIRECCIÓN INSTITUCIONAL

Institución: Dirección: Magallanes 910 / 11200 / Montevideo / Montevideo
Teléfono: (5982) 24102415
Correo electrónico/Sitio Web:viola@fing.edu.uy

Formación

Formación académica

CONCLUIDA

DOCTORADO

(1990 - 1995)

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

MAESTRÍA

(1988 - 1989)

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

GRADO

(1982 - 1986)

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

Idiomas

Español

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

Inglés

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

Francés

Entiende bien / Habla regular / Lee bien / Escribe regular

Italiano

Entiende regular / Habla regular / Lee bien / Escribe regular

Portugués

Entiende regular / Habla regular / Lee bien / Escribe regular

Areas de actuación

CIENCIAS NATURALES Y EXACTAS

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

CIENCIAS NATURALES Y EXACTAS

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

CIENCIAS NATURALES Y EXACTAS

Ciencias de la Computación e Información /Ciencias de la Computación /criptografia

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 /Ciencia de Datos - Inteligencia Artificial

Actuación profesional

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

Área Informática (PEDECIBA)

VÍNCULOS CON LA INSTITUCIÓN

Colaborador (03/2008 - 10/2023)

Investigador Honorario Grado 5 40 horas semanales
Area Informática

Colaborador (03/2001 - 03/2008)

Investigador Honorario Grado 4 40 horas semanales
Area de Inforática

Colaborador (03/1996 - 03/2001)

Investigador Honorario Grado 3 40 horas semanales
Area de Informática

ACTIVIDADES

GESTIÓN ACADÉMICA

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

Gestión de la Investigación

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

Participación en consejos y comisiones

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

Gestión de la Investigación

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

Gestión de la Investigación

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

Gestión de la Investigación

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

Facultad de Ingeniería / Instituto de Computación

VÍNCULOS CON LA INSTITUCIÓN

Funcionario/Empleado (02/2003 - 10/2023)

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

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

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

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

40 horas semanales
Escalafón: Docente
Grado: Grado 4
Cargo: Efectivo

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

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

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

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

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

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

ACTIVIDADES

LÍNEAS DE INVESTIGACIÓN

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

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

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

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 cienticos 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.
10 horas semanales , Coordinador o Responsable
Equipo: A. MARTÍN , F. FERNÁNDEZ
Areas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / analisis de algoritmos
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / combinatoria

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

Desarrollo de un grupo de investigación sólido y de relevancia internacional en Teoría de la Información, en colaboración con el grupo de Teoría de la Información de los laboratorios HP, California. Cuenta con la colaboración de docentes del Instituto de Ingeniería Eléctrica. Se han dictado cursos de posgrado, organizado visitas, hecho pasantías en los laboratorios HP, orientado

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.
10 horas semanales , Coordinador o Responsable
Equipo: A. MARTÍN , F. FERNÁNDEZ , N. CARRASCO , M. HERNÁNDEZ
Areas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Teoría de la Información

Criptografía (03/1998 - a la fecha)

Formar estudiantes de grado y posgrado en temas relacionados con criptografía en particular con aplicaciones a transacciones financieras. Se dirigieron 7 proyectos de grado en esta dirección preparando a estudiantes para realizar un trabajo apropiado en su tarea profesional, con especial énfasis a las telecomunicaciones. Este objetivo (iniciado ya en 1998), junto con todo el trabajo realizado en el área de Teoría de la Información (en colaboración con los laboratorios HP California, iniciado en 2000), apunta a formar recursos humanos capacitados en temas criptográficos y sus aplicaciones a las telecomunicaciones. La idea inicial era formar un grupo interdisciplinario que pudiera realizar además de trabajos de investigación, asesoramiento a empresas públicas como ANTEL. Lamentablemente, debido a muchas circunstancias desafortunadas, este plan se vio truncado por interferencia muy fuerte de autoridades de Facultad y otros grupos en otros lugares de Facultad que pretenden realizar estas tareas sin contar con los antecedentes de nuestro grupo de investigación. Es importante recalcar que no tengo la más mínima intención de integrarme a dichas iniciativas, 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.
10 horas semanales , Coordinador o Responsable
Equipo: A. MARTÍN , F. FERNÁNDEZ , N. CARRASCO , M. HERNÁNDEZ
Areas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / criptografia

Bioinformática (01/2006 - a la fecha)

Debido a una enfermedad crónica que tengo, y a un hecho familiar muy doloroso originado por la misma enfermedad, he empezado contactos con diversos grupos (relacionados con neurociencias) del Instituto de Investigaciones Biológicas Clemente Estable para realizar investigación conjunta. Aún no hemos realizado actividades conjuntas de colaboración, pero esperamos que podamos 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.
2 horas semanales , Coordinador o Responsable
Equipo:
Areas de conocimiento:

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

Ciencia de Datos e Inteligencia Artificial (02/2020 - 10/2023)

Es una actividad en la cual he venido colaborando internacionalmente por mucho tiempo. Se consolida en este momento por estar codirigiendo la tesis de doctorado de Bruno Scarone junto con Ricardo Baeza-Yates en Northeastern University (Boston).
Mixta , Coordinador o Responsable
Equipo: VIOLA, A. , SCARONE, B.

PROYECTOS DE INVESTIGACIÓN Y DESARROLLO

Randomness and Probabilsitic Analysis of Algorithms (RaPA2) (12/2019 - a la fecha)

Proyecto STIC-AMSUD en colaboración con Francia y Argentina.
10 horas semanales
Investigación
Coordinador o Responsable
En Marcha
Alumnos encargados en el proyecto:
Pregrado:5
Maestría/Magister:2
Doctorado:1
Financiación:
Agencia Nacional de Investigación e Innovación, Uruguay, Cooperación
Equipo: Alfredo VIOLA DEAMBROSIS
Palabras clave: combinatoria analítica aleatoriedad análisis dinámico de algoritmos criptografía funciones Booleanas
Areas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación e Información /

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

Red de colaboración con científicos chilenos y franceses financiado por el INRIA-Chile.
5 horas semanales
Universidad de Chile , Red internacional sobre voto electrónico
Investigación
Integrante del Equipo
En Marcha
Equipo:
Palabras clave: Voto Electrónico

EPAA - Entropy and probabilistic analysis of algorithms (09/2023 - a la fecha)

Proyecto STIC-AMSUD
5 horas semanales
Investigación
Integrante del Equipo
En Marcha
Equipo: VIOLA, A. , EDUARDO A. CANALE (Responsable) , C. Qureshi

NEW CRYPTO TOOLS - Nuevas herramientas criptográficas para la e-comunidad (04/2022 - a la fecha)

RED CYTED. El objetivo general de la propuesta consiste en desarrollar y/o mejorar primitivas criptográficas que no hayan sido implementadas de forma masiva en aplicaciones prácticas. La mayoría de esas primitivas son para la criptografía pos-cuántica, en vista a preparar la implementación segura de esas técnicas para el día en que los avances de la computación cuántica puedan poner en riesgo los sistemas actuales. Por otro lado, otros de los objetivos específicos se han propuesto para hacer más práctico y eficiente el uso de algunas variantes de los sistemas más comúnmente utilizados hoy en día, pero cuya utilización ha sido limitada por razones técnicas. Todos esos avances pueden tener un gran impacto en la vida cotidiana, especialmente en el contexto de la pandemia del Covid 19, con el aumento del uso de telecomunicaciones, comercio sin efectivo, comercio electrónico, votaciones electrónicas, etc, que requieren herramientas criptográficas más seguras y veloces.
5 horas semanales
Investigación

Integrante del Equipo
Concluido
Equipo: VIOLA, A. , EDUARDO A. CANALE , C. Qureshi (Responsable)

Análisis probabilístico de problemas relacionados con criptografía y comunicaciones (04/2019 - a la fecha)

Proyecto CSIC I+D
15 horas semanales
Facultad de Ingeniería , Instituto de Computación
Investigación
Coordinador o Responsable
En Marcha
Alumnos encargados en el proyecto:
Pregrado:3
Maestría/Magister:2
Financiación:
Comisión Sectorial de Investigación Científica, Uruguay, Apoyo financiero
Equipo: Alfredo VIOLA DEAMBROSIS , Alfredo Viola (Responsable)
Palabras clave: combinatoria analítica criptografía comunicaciones
Areas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación /

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

Proyecto STIC-AMSUD con participación de investigadores de la Universidad de Caen y Paris 7 (Francia) y de la Universidad Nacional General Sarmiento (Argentina).
5 horas semanales
STIC-AMSUD
Investigación
Coordinador o Responsable
En Marcha
Alumnos encargados en el proyecto:
Pregrado:2
Doctorado:1
Financiación:
Agencia Nacional de Investigación e Innovación, Uruguay, Cooperación
Equipo:
Palabras clave: criptografía Combinatoria Análisis dinámico de algoritmos
Areas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Análisis Dinámico de Algoritmos

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

Proyecto de Investigación CSIC con la participación de 2 estudiantes de grado, 1 estudiante de Maestría y un estudiante interesado en ingresar al doctorado.
10 horas semanales
Universidad de la República , CSIC I+D
Investigación
Coordinador o Responsable
En Marcha
Alumnos encargados en el proyecto:
Pregrado:2
Maestría/Magister:1
Doctorado:1
Equipo: SILVEIRA, A. , FONSECA, S. , ROTNDO, P.
Palabras clave: Combinatoria Analítica

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

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

Coordinador o Responsable
Concluido
Alumnos encargados en el proyecto:
Pregrado:1
Maestría/Magister:2
Equipo: CARRASCO , FERNÁNDEZ , FONSECA
Palabras clave: Análisis de Algoritmos sistemas dinámicos
Areas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / combinatoria analítica

Boole (07/2010 - 07/2013)

Proyecto ANR frances, con la participación de varios de mis coautores. Una parte importante del proyecto se basó en temas relacionados con mis trabajos en funciones Booleanas. Yo he sido invitado varias veces a participar de reuniones científicas en Francia, como investigador invitado, en el marco de este proyecto. He dato tambien varias charlas.
1 horas semanales
ANR Project BOOLE; ANR-09-BLAN-0011
Investigación
Otros
Concluido
Financiación:
Institución del exterior, Apoyo financiero
Equipo: VIOLA
Palabras clave: funciones booleanas
Areas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / combinatoria analítica

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

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.
2 horas semanales
Investigación
Integrante del Equipo
En Marcha
Alumnos encargados en el proyecto:
Pregrado:2
Maestría/Magister:1
Financiación:
Institución del exterior, Apoyo financiero
Equipo: R. MOTZ (Responsable)

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

Programa ECOS de cooperación francesa con la Universidad de París XIII y la Universidad de Caen
5 horas semanales
ECOS
Investigación
Coordinador o Responsable
En Marcha
Alumnos encargados en el proyecto:
Pregrado:1
Maestría/Magister:1
Equipo: G. SEROUSSI , F. BASSINO , J. CLÉMENT , B. VALLÉE , N. CARRASCO , M. HERNÁNDEZ
Palabras clave: funciones booleanas Teoría de la Información criptografía Combinatoria
Areas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / criptografia
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / combinatoria

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

Programa de cooperación STIC-AMSUD con investigadores de Francia, Brasil y Chile. The overall goal 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.
5 horas semanales
STIC-AMSUD
Investigación
Integrante del Equipo
Concluido
Alumnos encargados en el proyecto:
Pregrado:1
Maestría/Magister:1
Equipo: M. HERNÁNDEZ , G. BETARTE , C. LUNA , F. ZIPITRÍA , T. REZK (Responsable) , R. DAHAB , A. HEVIA
Palabras clave: criptografía seguridad de la información
Areas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / criptografia

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

Proyecto de Investigación CSIC en conjunto con investigadores de las Universidades de Caen y Paris XIII (Francia)
10 horas semanales
CSIC
Investigación
Coordinador o Responsable
Concluido
Alumnos encargados en el proyecto:
Pregrado:1
Maestría/Magister:1
Financiación:
Comisión Sectorial de Investigación Científica, Uruguay, Apoyo financiero
Equipo: N. CARRASCO , M. HERNÁNDEZ , G. SEROUSSI , F. BASSINO , J. CLÉMENT
Palabras clave: funciones booleanas criptografía
Areas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / combinatoria
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / criptografia
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Teoría de la Información

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

Proyecto PDT, con participación de investigadores de Francia y de los laboratorios HP, California
10 horas semanales
Investigación
Coordinador o Responsable
Concluido
Alumnos encargados en el proyecto:
Maestría/Magister:1
Equipo: F. FERNÁNDEZ , G. SEROUSSI , F. BASSINO , J. CLÉMENT , A. VIOLA (Responsable)

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

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

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

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

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

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

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

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

DOCENCIA

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

Doctorado

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

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

Maestría

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

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

Grado
Responsable
Asignaturas:
Teoría de la Computación, 12 horas, Teórico-Práctico
Areas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación /

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

Grado
Responsable
Asignaturas:
Combinatoria Analítica, 15 horas, Teórico-Práctico
Areas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación /

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

Grado
Asistente
Asignaturas:
Programación 3, 5 horas, Teórico

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

Maestría
Responsable
Asignaturas:
Fundamentos de Criptografía, 18 horas, Teórico-Práctico
Areas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación /

Ingeniería en Computación (03/2013 - a la fecha)

Grado
Responsable
Asignaturas:
Criptografía, 15 horas, Teórico-Práctico
Areas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación /

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

Grado

Asignaturas:
Programación 3, 6 horas, Teórico-Práctico

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

Grado

Asignaturas:
Programación III (Plan 85), 6 horas, Teórico-Práctico
Programacion II (Plan 85), 6 horas, Teórico-Práctico

Ingeniería Eléctrica (01/1987 - 06/1988)

Grado

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

EXTENSIÓN

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

5 horas

(06/2010 - a la fecha)

PEDECIBA/Plan Ceibal
3 horas
Areas de conocimiento:
Ciencias Naturales y Exactas / Otras Ciencias Naturales / Otras Ciencias Naturales / Divulgación científica de todas las áreas del Pedeciba

Edición de video "Investigando en Binario con los dedos", en el marco del programa "Investigando con ..." en cojunto del PEDECIBA, ANEP y Plan Ceibal (04/2019 - a la fecha)

5 horas

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

2 horas

Asesoramiento al Parlamento Nacional en relacion a leyes sobre comercio electronico (colaboracion con Facultad de Derecho) (03/2000 - 06/2002)

5 horas

GESTIÓN ACADÉMICA

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

Gestión de la Investigación

Miembro suplente de la Comisión de Instituto (11/2014 - 11/2018)

Facultad de Ingeniería, Instituto de Computación
Participación en cogobierno 2 horas semanales

Miembro suplente de comisión de instituto de computación (02/2015 - 11/2018)

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

Miembro suplente de la Comisión de Instituto de Computación. (11/2014 - 11/2018)

Facultad de Ingeniería, Instituto de Computación
Participación en cogobierno 5 horas semanales
Areas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación e Información /

Participación en Comisión de Planes de Estudio del Claustro. (07/2014 - 07/2018)

Facultad de Ingeniería Gestión de la Enseñanza 5 horas semanales

Miembro de la Comisión de Planes de Estudio del Claustro (11/2014 - 04/2018)

Gestión de la Enseñanza

Miembro Alterno de la Comisión Academica de Posgrado de la Facultad de Ingeniería (08/2005 - 09/2014)

Gestión de la Investigación

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

Participación en cogobierno

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

Participación en consejos y comisiones

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

Gestión de la Investigación

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

Participación en cogobierno

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

Participación en cogobierno

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

Participación en cogobierno

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

Participación en cogobierno

SECTOR EXTRANJERO/INTERNACIONAL/OTROS - ESPAÑA

Universidad Politécnica de Catalunya*

VÍNCULOS CON LA INSTITUCIÓN

Profesor visitante (09/2022 - 12/2022)

Año Sabático 40 horas semanales
Visita como parte de mi año sabático.

Profesor visitante (05/2015 - 06/2015)

40 horas semanales

Profesor visitante (06/2014 - 06/2014)

40 horas semanales

Profesor visitante (05/2013 - 06/2013)

40 horas semanales

Profesor visitante (09/2011 - 08/2012)

Año sabàtico 40 horas semanales
Usufructuo de año sabàtico

Profesor visitante (06/2009 - 06/2009)

40 horas semanales
Dictado de un curso de maestría y doctorado en Teoría de Códigos

Profesor visitante (07/2008 - 07/2008)

40 horas semanales
Departamento de Lenguajes y Sistemas Informáticos

Profesor visitante (04/2004 - 04/2004)

40 horas semanales
Departamento de Lenguajes y Sistemas Informáticos

Profesor visitante (07/2001 - 07/2001)

40 horas semanales
Departamento de Lenguajes y Sistemas Informáticos

Profesor visitante (11/2000 - 11/2000)

40 horas semanales
Departamento de Lenguajes y Sistemas Informáticos

Profesor visitante (07/1997 - 07/1997)

40 horas semanales
Departamento de Lenguajes y Sistemas Informáticos

ACTIVIDADES

DOCENCIA

(07/2001 - 07/2011)

Doctorado
Invitado
Asignaturas:
Anàlisis de algoritmos de ordenaciòn y bùsqueda, 6 horas, Teórico-Práctico

(06/2009 - 06/2009)

Doctorado

Asignaturas:
Introducciòn a la Teorìa de Còdigos, 6 horas, Teórico-Práctico

(07/2008 - 07/2008)

Doctorado
Invitado
Asignaturas:
Introducciòn a la Teorìa de Còdigos, 6 horas, Teórico-Práctico

SECTOR EXTRANJERO/INTERNACIONAL/OTROS - FRANCIA

Universite de Caen

VÍNCULOS CON LA INSTITUCIÓN

Profesor visitante (06/2018 - 07/2018)

40 horas semanales

Profesor visitante (07/2017 - 07/2017)

40 horas semanales

Profesor visitante (06/2015 - 06/2015) Trabajo relevante

40 horas semanales

Profesor visitante (06/2014 - 06/2014)

40 horas semanales

Profesor visitante (06/2013 - 06/2013)

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

Profesor visitante (06/2010 - 07/2010)

40 horas semanales

Profesor visitante (07/2009 - 07/2009)

40 horas semanales

Profesor visitante (06/2008 - 07/2008)

40 horas semanales
Departamento de Computación

Profesor visitante (06/2007 - 06/2007)

40 horas semanales
Departamento de Computación

SECTOR EXTRANJERO/INTERNACIONAL/OTROS - FRANCIA

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

VÍNCULOS CON LA INSTITUCIÓN

Profesor visitante (06/2017 - 06/2017)

40 horas semanales

Profesor visitante (05/2010 - 05/2010)

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

SECTOR EXTRANJERO/INTERNACIONAL/OTROS - CHILE

Universidad de Chile

VÍNCULOS CON LA INSTITUCIÓN

Profesor visitante (11/2016 - 11/2016)

40 horas semanales
Visita científica a Patricio Poblete y Alejandro Hevia

Profesor visitante (12/2012 - 12/2012)

40 horas semanales

Profesor visitante (12/2009 - 12/2009)

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

Profesor visitante (12/2007 - 12/2007)

40 horas semanales
NIC Chile

Profesor visitante (12/2006 - 12/2006)

40 horas semanales
NIC Chile

Profesor visitante (12/2000 - 12/2000)

40 horas semanales
Departamento de Ciencias de la Computación

Profesor visitante (12/1999 - 12/1999)

40 horas semanales
Departamento de Ciencias de la Computación

Profesor visitante (12/1998 - 12/1998)

40 horas semanales
Departamento de Ciencias de la Computación

Profesor visitante (12/1997 - 12/1997)

40 horas semanales
Departamento de Ciencias de la Computación

Profesor visitante (12/1996 - 12/1996)

40 horas semanales
Departamento de Ciencias de la Computación

SECTOR EXTRANJERO/INTERNACIONAL/ENSEÑANZA SUPERIOR - CANADÁ

University of Waterloo

VÍNCULOS CON LA INSTITUCIÓN

Profesor visitante (07/2015 - 07/2015)

40 horas semanales

Profesor visitante (06/2001 - 06/2001)

40 horas semanales
Departamento de Computación

Profesor visitante (05/1997 - 06/1997)

40 horas semanales
Departamento de Computación

Profesor visitante (09/1996 - 09/1996)

40 horas semanales
Departamento de Computación

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

Teacher Assistant 5 horas semanales

SECTOR EXTRANJERO/INTERNACIONAL/ENSEÑANZA SUPERIOR - FRANCIA

Universite de Paris VII

VÍNCULOS CON LA INSTITUCIÓN

Profesor visitante (06/2015 - 06/2015)

40 horas semanales

SECTOR EXTRANJERO/INTERNACIONAL/ENSEÑANZA SUPERIOR - FRANCIA

Universite de Paris XIII (Paris-Nord)

VÍNCULOS CON LA INSTITUCIÓN

Colaborador (11/2003 - 11/2010)

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

Profesor visitante (05/2010 - 05/2010)

40 horas semanales
Investigación conjunta con la Dr. Frédérique Bassino

Profesor visitante (05/2006 - 06/2006)

40 horas semanales
Laboratorio de Informática (LIPN)

Profesor visitante (06/2003 - 11/2003)

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

SECTOR EXTRANJERO/INTERNACIONAL/OTROS - ALEMANIA

Universitat Bonn

VÍNCULOS CON LA INSTITUCIÓN

Profesor visitante (06/2010 - 06/2010)

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

Profesor visitante (07/2007 - 07/2007)

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

SECTOR EXTRANJERO/INTERNACIONAL/OTROS - CANADÁ

Carleton University

VÍNCULOS CON LA INSTITUCIÓN

Profesor visitante (05/2009 - 05/2009)

40 horas semanales
Investigación conjunta y participación en dos eventos científicos

Profesor visitante (04/2004 - 04/2004)

40 horas semanales
Departamento de Matemáticas

Profesor visitante (07/2002 - 07/2002)

40 horas semanales
Departamento de Matemáticas

Profesor visitante (06/2001 - 06/2001)

40 horas semanales
Departamento de Matemáticas

SECTOR EXTRANJERO/INTERNACIONAL/OTROS - BRASIL

Universidad Estadual de Campinas

VÍNCULOS CON LA INSTITUCIÓN

Profesor visitante (05/2009 - 05/2009)

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

SECTOR EXTRANJERO/INTERNACIONAL/OTROS - FRANCIA

Université de Marne la Vallée

VÍNCULOS CON LA INSTITUCIÓN

Profesor visitante (07/2008 - 07/2008)

40 horas semanales
Instituto Gaspard Monge

Profesor visitante (07/2007 - 07/2007)

40 horas semanales
Instituto Gaspard Monge

Profesor visitante (05/2005 - 06/2005)

40 horas semanales
Instituto Gaspard Monge

SECTOR EXTRANJERO/INTERNACIONAL/OTROS - FRANCIA

Institut National de Recherche en Informatique et Automatique

VÍNCULOS CON LA INSTITUCIÓN

Profesor visitante (06/2007 - 06/2007)

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

Profesor visitante (06/2002 - 06/2002)

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

SECTOR EXTRANJERO/INTERNACIONAL/OTROS - ESTADOS UNIDOS

Hewlett-Packard Laboratories

VÍNCULOS CON LA INSTITUCIÓN

Profesor visitante (01/2007 - 01/2007)

40 horas semanales
Grupo de Teoría de la Información

Profesor visitante (06/2004 - 06/2004)

40 horas semanales
Grupo de Teoría de la Información

Profesor visitante (01/2002 - 01/2002)

40 horas semanales
Grupo de Teoría de la Información

CARGA HORARIA

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

Producción científica/tecnológica

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

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

Uno de mis trabajos fundamentales está precisamente relacionado con la resolución de un problema de

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

Producción bibliográfica

ARTÍCULOS PUBLICADOS

ARBITRADOS

Asymptotic analysis and efficient random sampling of directed ordered acyclic graphs (Completo, 2023)

VIOLA, A. , PÉPIN,M
Electronic Journal of Combinatorics, 2023
Medio de divulgación: Internet
ISSN: 10971440
E-ISSN: 1077-8926
https://arxiv.org/abs/2303.14710
Puse publicado porque lo tenemos en el ArXiv y está aún en proceso de evaluación. No sé cómo poner artículos que están en proceso de evaluación.

A perspective on theoretical computer science in Latin America. (Completo, 2020)

VIOLA, A. , KIWI, M , Kohayakawa, Y. , Sergio Rajsbaum, , Francisco Rodríguez-Henríquez , Jayme Luiz Szwarcfiter
Communications of the ACM, v.: 63 11 , p.:102 - 107, 2020
Medio de divulgación: Internet
ISSN: 00010782
E-ISSN: 15577317
https://repositorio.uchile.cl/bitstream/handle/2250/179570/A-Perspective-on-Theoretical-Computer-Sci
Scopus® WEB OF SCIENCE™

A technological and innovative approach to COVID-19 in Uruguay (Completo, 2020)

VIOLA, A. , MILANO,G , VALLESPIR, D.
Communications of the ACM, v.: 63 11 , p.:53 - 55, 2020
Medio de divulgación: Internet
ISSN: 00010782
E-ISSN: 15577317
https://cacm.acm.org/magazines/2020/11/248204-a-technological-and-innovative-approach-to-covid-19-in
Scopus WEB OF SCIENCE™

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

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

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

SVANTE JANSON , VIOLA, A.
Algorithmica, v.: 75 p.:1 - 58, 2016
Palabras clave: hashing
Areas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / combinatoria analítica
Medio de divulgación: Internet
ISSN: 01784617
E-ISSN: 14320541
Considero que es el mejor trabajo de mi carrera científica.
Scopus WEB OF SCIENCE™

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

BASSINO, F , CLÉMENT, J , SEROUSSI, G , VIOLA, A.
IEEE Transactions on Information Theory, v.: 59 4 , p.:2375 - 2395, 2013
Palabras clave: Códigos de prefijos óptimos alfabetos infinitos distribución geométrica bidimensional
Areas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Teoría de la Información
Medio de divulgación: Papel
ISSN: 00189448
E-ISSN: 15579654
Scopus WEB OF SCIENCE™

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

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

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

GATHEN J. , ZIEGLER K. , VIOLA, A.
SIAM Journal on Discrete Mathematics, v.: 27 2 , p.:855 - 891, 2013
Areas de conocimiento:

Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / analisis de algoritmos
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / cuerpos finitos
ISSN: 08954801
E-ISSN: 10957146
Scopus WEB OF SCIENCE™

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

D. VERGNAUD , VIOLA, A.
Finite Fields and Their Applications, 2011
Palabras clave: polynomials over finite fields
Areas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / criptografia
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / cuerpos finitos
ISSN: 10715797
E-ISSN: 10902465
Scopus WEB OF SCIENCE™

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

A. HEVIA , P. POBLETE , VIOLA, A.
Theoretical Computer Science, 2011
Palabras clave: DC Nets
Areas de conocimiento:
Ciencias Naturales y Exactas / Matemáticas / Matemática Aplicada / Criptografía
Ciencias Naturales y Exactas / Matemáticas / Matemática Aplicada / Combinatoria
ISSN: 03043975
Scopus WEB OF SCIENCE™

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

DEVROYE, L , VIOLA, A.
Information Processing Letters, 2011
Palabras clave: linear probing hashing Longest Probe
Areas de conocimiento:
Ciencias Naturales y Exactas / Matemáticas / Matemática Aplicada / Probabilistic Analysis of Algorithms
ISSN: 00200190
Scopus WEB OF SCIENCE™

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

LE BARS, J. M. , VIOLA, A.
IEEE Transactions on Information Theory, v.: 56 3 , p.:1247 - 1261, 2010
Palabras clave: funciones inmunes a la correlación funciones booleanas 1-resilientes
Areas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Funciones booleanas, criptografía
Medio de divulgación: Papel
ISSN: 00189448
E-ISSN: 15579654
Scopus WEB OF SCIENCE™

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

VIOLA, A.
Discrete Mathematics & Theoretical Computer Science, v.: 12 2 , p.:307 - 332, 2010
Palabras clave: linear probing hashing with buckets Parking Problem
Areas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la

Computación / analisis de algoritmos
E-ISSN: 13658050
www.dmtcs.org/dmtcs-ojs/index.php/dmtcs/article/download/1359/2918
Considero que es el mejor trabajo de mi carrera científica hasta el momento. Número especial dedicado a los 60 años de Philippe Flajolet, miembro de la Academia de Ciencias Francesa, y el líder mundial en el área de Análisis de Algoritmos. En 1998 resolví un problema abierto que aparece en el tercer volumen de la colección "The Art of Computer Programming" de Donald Erwin Knuth. Esta es la colección más vendida y leída en la historia de la Computación.Este problema ("linear probing hashing") fue el primer problema que D. Knuth analizó en 1962 y dio origen a esta colección de libros. Además este análisis es considerado como el punto inicial de la creación del área de investigación Análisis de Algoritmos. En este trabajo, generalizo dicho análisis, dando la distribución completa del costo de búsqueda de un elemento aleatorio (en el libro sólo se pedía por el valor esperado), y además resuelvo dos problemas muy importantes que estaban sin resolver. El primero es la 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".
Scopus

Adaptive Sampling Strategies for Quickselect (Completo, 2010)

MARTÍNEZ, C , PANARIO, D , VIOLA, A.
ACM Transactions on Algorithms, v.: 6 3 , 2010
Palabras clave: algoritmos de seleccion
Areas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / analisis de algoritmos
Medio de divulgación: Papel
Lugar de publicación: Articulo 53
ISSN: 15496325
E-ISSN: 15496333
http://talg.acm.org/
Scopus WEB OF SCIENCE™

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

VIOLA, A.
ACM Transactions on Algorithms, v.: 1 2 , p.:214 - 242, 2005
Palabras clave: linear probing hashing Exact Distribution
Areas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / analisis de algoritmos
Medio de divulgación: Papel
ISSN: 15496325
E-ISSN: 15496333
http://talg.acm.org/

On worst case Robin Hood Hashing (Completo, 2004)

DEVROYE, L , MORIN, P , VIOLA, A.
SIAM Journal on Computing, v.: 33 4 , p.:923 - 936, 2004
Palabras clave: Robin Hood Hashing
Areas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / ontologías
Medio de divulgación: Papel
ISSN: 00975397
E-ISSN: 10957111
http://epubs.siam.org/sam-bin/dbq/article/40337
Scopus WEB OF SCIENCE™

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

PANARIO, D , PITTEL, B , RICHMOND, B , VIOLA, A.
Random Structures and Algorithms, v.: 19 3-4 , p.:525 - 551, 2001
Palabras clave: polinomios sobre cuerpos finitos

Areas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / analisis de algoritmos
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / criptografia
Medio de divulgación: Papel
ISSN: 10429832
E-ISSN: 10982418
http://www3.interscience.wiley.com/cgi-bin/issuetoc?ID=88510505
Scopus WEB OF SCIENCE™

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

VIOLA, A. , POBLETE, P
Algorithmica, v.: 21 1 , p.:37 - 71, 1998
Palabras clave: linear probing hashing with buckets
Areas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / analisis de algoritmos
Medio de divulgación: Papel
ISSN: 01784617
E-ISSN: 14320541
http://www.informatik.uni-trier.de/~ley/db/journals/algorithmica/algorithmica21.html
En este trabajo se resuelve un problema abierto de nivel 48 del libro 3 de la colección The Art of Computer Programming" de D. Knuth. En particular generaliza los resultados del primer análisis hecho por D. Knuth en su vida en 1962 y que dio origen al área de Análisis de Algoritmos y fue su inspiración para iniciar esta famosa colección de volúmenes. Este trabajo además fue el origen de varias correspondencias epistolares y por e-mail (que documento) con D. Knuth que culminaron con el paper On the Analysis of Linear Probing Hashing" indicado más arriba en conjunto con el paper de D. Knuth ``Linear Probing and Graphs" que aparece en el mismo volumen.
Scopus WEB OF SCIENCE™

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

FLAJOLET, P , POBLETE, P , VIOLA, A.
Algorithmica, v.: 22 4 , p.:490 - 515, 1998
Palabras clave: linear probing hashing
Areas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / analisis de algoritmos
Medio de divulgación: Papel
ISSN: 01784617
E-ISSN: 14320541
http://www.informatik.uni-trier.de/~ley/db/journals/algorithmica/algorithmica22.html
Scopus WEB OF SCIENCE™

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

POBLETE, P , VIOLA, A. , MUNRO, I
Random Structures and Algorithms, v.: 10 2 , p.:221 - 255, 1997
Palabras clave: linear probing hashing Diagonal Poisson Transform
Areas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / analisis de algoritmos
Medio de divulgación: Papel
ISSN: 10429832
E-ISSN: 10982418
http://www3.interscience.wiley.com/cgi-bin/issuetoc?ID=69000567
Scopus WEB OF SCIENCE™

LIBROS

Selected papers LATIN 2014 (Compilación Revista , 2015)

VIOLA, A.
Publicado

Número de volúmenes: 200
Número de páginas: 300
Tipo de puplicación: Investigación
Referado
Palabras clave: Teoría de la Computación
Areas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Teoría de la Computación
Medio de divulgación:
ISSN/ISBN:
Financiación/Cooperación:
Facultad de Ingeniería - UDeLaR / Otra, Uruguay

Proceedings LATIN 2014 (Compilación Libro , 2014)

PARDO, A. , VIOLA, A.
Publicado
Número de volúmenes: 150
Número de páginas: 767
Palabras clave: Teoría de la Computación
Areas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación /
Medio de divulgación:
ISSN/ISBN:

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

LóPEZ-ORTIZ, A. , BRODNIK,A , RAMAN,V , VIOLA, A.
Publicado
Número de volúmenes: 150
Número de páginas: 362 , 8066
Editorial: LNCS - SPRINGER
Palabras clave: Algorithms
Areas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación /
Medio de divulgación:
ISSN/ISBN:

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

VIOLA, A.
Publicado
Palabras clave: hashing
Areas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / combinatoria analítica
Medio de divulgación:
ISSN/ISBN:
Es la introducción del capítulo sobre hashing en la colección completa de los trabajos de Philippe Flajolet. Philippe Flajolet, miembro de la academia de ciencias francesa, fue el líder de nuestra comunidad científica, y desarrolló los fundamentos del área de Combinatoria Analítica. Falleció en marzo 2011, y se está editando una colección completa de su trabajo científico. Se nos 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.

Capítulos:
Introduction to the chapter «Philippe Flajolet and his contribution to the analysis of hashing problems«.
Organizadores: Mark Ward, Robert Sedgewick, Bruno Salvy, Philippe Flajolet, Michele Soria, Brigite Vallee, Hsien-Kuei Hwang
Página inicial 355, Página final 360

Proceedings LATIN 2000 (Compilación Compilación , 2000)

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

Publicado
Número de volúmenes: 150
Número de páginas: 484 , 1776
Editorial: LNCS - SPRINGER
Palabras clave: Teoría de la Computación
Areas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación /
Medio de divulgación:
ISSN/ISBN: 3540673067

PUBLICACIÓN DE TRABAJOS PRESENTADOS EN EVENTOS

Qubo model for the Closest Vector Problem (2023)

VIOLA, A. , C. Qureshi , EDUARDO A. CANALE
Publicado
Resumen expandido
Evento: Internacional
Descripción: Central European Conference on Cryptology
Ciudad: Linz
Año del evento: 2023
Publicación arbitrada
Medio de divulgación: Internet
https://arxiv.org/abs/2304.03616

Unbiased Similarity Estimators Using Samples (2023)

VIOLA, A. , MARTÍNEZ,C
Publicado
Resumen expandido
Evento: Internacional
Descripción: 16th International Conference on Similarity Search and Applications, SISAP 2023
Ciudad: La Coruña
Año del evento: 2023
Publicación arbitrada
Medio de divulgación: Internet
https://www.sisap.org/2023/posters/3085.pdf

Unlabelled ordered DAGs and labelled DAGs: constructive enumeration and uniform random sampling. (2021)

VIOLA, A. , PÉPIN, M , GENITRINI, A
Publicado
Resumen expandido
Evento: Internacional
Descripción: LAGOS 2021
Ciudad: San Pablo
Año del evento: 2021
Anales/Proceedings:Proceeding LAGOS 2021
Pagina inicial: 468
Pagina final: 477
Publicación arbitrada
Medio de divulgación: Internet
https://eventos.ufabc.edu.br/lagos2021/
Este artículo fue realizado en el marco de los estudios de doctorado de Martin Pépin.

Uruguayan Cryptography: Printed Book Covers (2019)

VIOLA, A. , CASTRO, F. , GATHEN, J. , CABEZAS, J.J. , TISCORNIA, J.
Publicado
Resumen expandido
Evento: Internacional
Descripción: Histocrypt 2019
Ciudad: Mons, Bélgica
Año del evento: 2019
Anales/Proceedings:Proceedings of the 2nd International Conference on Historical Cryptology, HistoCrypt 2019, June 23-26, 2019, Mons, Belgium

Publicación arbitrada
Palabras clave: desencriptado mln tapa libro EVA.
Areas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación e Información / criptografía
Medio de divulgación: Internet
Financiación/Cooperación:
Facultad de Ingeniería / Otra, Uruguay
http://www.ep.liu.se/ecp/contents.asp?issue=158
Es un trabajo relacionado con el desencriptado de un mensaje enviado por miembros del MLN en Suecia al Penal de Libertad a principio de los años '80 codificado en la tapa del libro llamado EVA. Este trabajo es la base para la tesis de Maestría de Francisco Castro, en codirección entre Alfredo Viola y Joachim von zur Gathen (Universidad de Bonn).

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

VIOLA, A. , BODINI, Olivier , DIEN, Matthieu , GENITRINI, Antoine
Publicado
Resumen expandido
Evento: Internacional
Descripción: Conference on Analysis of Algorithms 2018
Ciudad: Uppsala
Año del evento: 2018
Publicación arbitrada
http://math.uu.se/aofa2018

Analysis of the Continued Logarithm Algorithm (2018) Trabajo relevante

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

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

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

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

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

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

A unified approach to linear probing hashing (2014)

SVANTE JANSON , VIOLA, A.
Publicado
Resumen expandido
Evento: Internacional
Descripción: AofA 2014
Ciudad: París
Año del evento: 2014
Publicación arbitrada
Palabras clave: linear probing hashing
Areas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / combinatoria analítica

Beating the Birthday Paradox in Dining Cryptographer Networks (2014)

GARCÍA, P. , VAN DE GRAAF, J. , A. HEVIA , VIOLA, A.
Publicado
Resumen expandido
Evento: Internacional
Descripción: LATINCRYPT 2014
Ciudad: Florianópolis
Año del evento: 2014
Publicación arbitrada
Palabras clave: DC Nets
Areas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / criptografia
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / combinatoria analítica

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

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

Enumerative encoding of correlation immune Boolean functions (2011)

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

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

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

F. FERNÁNDEZ , VIOLA, A. , M WEINBERGER
Publicado
Resumen expandido
Evento: Internacional
Descripción: IEEE Data Compression Conference
Año del evento: 2010
Palabras clave: context sets
Areas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Estructuras de Datos
Ingeniería y Tecnología / Ingeniería Eléctrica, Ingeniería Electrónica e Ingeniería de la Información / Telecomunicaciones / Teoria de la Información

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

GATHEN J. , VIOLA, A. , ZIEGLER K.
Publicado
Resumen expandido
Evento: Internacional
Descripción: LATIN 2010
Ciudad: Oaxaca, Mexico
Año del evento: 2010
Publicación arbitrada
Palabras clave: polinomios sobre cuerpos finitos
Areas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / combinatoria
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / cuerpos finitos

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

LE BARS, J. M. , VIOLA, A.
Publicado
Completo
Evento: Internacional
Descripción: IEEE International Symposium on Information Theory
Año del evento: 2007
Palabras clave: funciones booleanas 1-resiliente
Areas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / criptografia
Medio de divulgación: Papel

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

BASSINO, F , CLÉMENT, J , SEROUSSI, G , VIOLA, A.
Publicado
Completo
Evento: Internacional
Descripción: ISIT - IEEE International Symposium of Information Theory
Año del evento: 2006

Palabras clave: Códigos de prefijos óptimos
Areas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Teoría de la Información
Medio de divulgación: Papel

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

BASSINO, F , CLÉMENT, J , SEROUSSI, G , VIOLA, A.
Publicado
Completo
Evento: Internacional
Descripción: DCC - IEEE Data Compression Conference
Año del evento: 2006
Palabras clave: Códigos de prefijos óptimos
Areas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Teoría de la Información
Medio de divulgación: Papel

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

VIOLA, A.
Publicado
Completo
Evento: Internacional
Descripción: First International Conference on Analysis of Algorithms
Año del evento: 2005
Palabras clave: Exact Distribution linear probing hashing with buckets
Areas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / 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.

Adaptive Sampling Strategies for Quickselect (2004)

MARTÍNEZ, C , PANARIO, D , VIOLA, A.
Publicado
Completo
Evento: Internacional
Descripción: ACM Symposium on Discrete Algorithms - SODA
Año del evento: 2004
Palabras clave: algoritmos de seleccion
Areas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / analisis de algoritmos
Medio de divulgación: Papel

Analysis of Quickfind with small subfiles (2002)

MARTÍNEZ, C , PANARIO, D , VIOLA, A.
Publicado
Completo
Evento: Internacional
Descripción: Colloquium on Mathematics and Computer Science: Algorithms, Trees, Combinatorics

and Probabilities
Ciudad: Versailles
Año del evento: 2002
Palabras clave: algoritmos de seleccion
Areas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / analisis de algoritmos
Medio de divulgación: Papel

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

POBLETE, P , VIOLA, A.
Publicado
Completo
Evento: Internacional
Descripción: First Brazilian Symposium on Graphs, Algorithms and Combinatorics - GRACO
Año del evento: 2001
Anales/Proceedings:Electronic Notes in Discrete Mathematics
Volumen:7
Palabras clave: Hashing Algorithms Deletions
Areas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / analisis de algoritmos
Medio de divulgación: Papel

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

PANARIO, D , VIOLA, A.
Publicado
Completo
Evento: Internacional
Descripción: Tercer Latin American symposium on Theoretical Informatics
Año del evento: 1998
Anales/Proceedings:Lecture Notes in Computer Science
Volumen:1380
Pagina inicial: 1
Pagina final: 10
Palabras clave: polinomios sobre cuerpos finitos tests de irreducibilidad
Areas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / analisis de algoritmos
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / criptografia
Medio de divulgación: Papel
http://www.informatik.uni-trier.de/~ley/db/conf/latin/latin98.html

Analysis of linear probing hashing with buckets (1996)

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

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

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

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

Learning Secondary Structure of Proteins (1994)

VIOLA, A. , LI, M
Publicado
Completo
Evento: Internacional
Descripción: 6th International Conference on Computing and Information
Año del evento: 1994
Palabras clave: estructura secundaria de proteinas
Areas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / bioinformática
Medio de divulgación: Papel

Producción técnica

TRABAJOS TÉCNICOS

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

Asesoramiento
VIOLA, A.
Colaborar en la propuesta de restructura de dicha CV y su viabilidad futura
País: República Dominicana
Idioma: Español
Disponibilidad: Restricta

Duración: 36 meses
Institución financiadora: Sin fines de lucro
Palabras clave: TICs y desarrollo social Sociedad de la Información
Areas de conocimiento:
Ingeniería y Tecnología / Ingeniería Eléctrica, Ingeniería Electrónica e Ingeniería de la Información / Ingeniería de Sistemas y Comunicaciones / Tecnologías de la Comunicación en Información
Medio de divulgación: Internet
http://funredes.org/mistica
Mi vínculo con MISTICA se originó cuando yo era miembro del SC de Eurolatis, cuando me puse en contacto con el director de la ONG FUNREDES, Daniel 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.

Tecnologías de la Información aplicadas a la Salud (2001)

Consultoría
VIOLA, A.
Asesor de la red Eurolatis para presentar proyectos en los programas marco de la Unión Europea
País: Cuba
Idioma: Español
Ciudad: La Habana
Disponibilidad: Restricta

Duración: 6 meses
Institución financiadora: Unión Europea
Palabras clave: TICs y desarrollo social Sociedad de la Información TICs y su uso en salud
Areas de conocimiento:
Ingeniería y Tecnología / Ingeniería Eléctrica, Ingeniería Electrónica e Ingeniería de la Información / Ingeniería de Sistemas y Comunicaciones / Tecnologías de la Comunicación en Información
Medio de divulgación: Internet
http://www.eurolatis.upm.es
Eurolatis era una red entre Europa y América Latina para el desarrollo de la Sociedad de la Información en nuestra región. La idea era organizar eventos coincidentes con los llamados en el programa marco de la Unión Europea a los efectos de presentar proyectos específicos en dichas convocatorias. Yo era miembro del Steering Committee por 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.

Tecnologías de la Información aplicadas a la Educación (2000)

Consultoría
VIOLA, A.
Asesor de la red Eurolatis para presentar proyectos en los programas marco de la Unión Europea
País: Chile
Idioma: Español
Ciudad: Santiago de Chile - Montevideo
Disponibilidad: Restricta

Duración: 6 meses
Institución financiadora: Unión Europea
Palabras clave: TICs y desarrollo social TICs y su uso en educación Sociedad de la Información
Areas de conocimiento:
Ingeniería y Tecnología / Ingeniería Eléctrica, Ingeniería Electrónica e Ingeniería de la Información / Ingeniería de Sistemas y Comunicaciones / Tecnologías de la Comunicación en Información
Medio de divulgación: Internet
http://www.eurolatis.upm.es
Eurolatis era una red entre Europa y América Latina para el desarrollo de la Sociedad de la Información en nuestra región. La idea era organizar eventos coincidentes con los llamados en el programa marco de la Unión Europea a los efectos de presentar proyectos específicos en dichas convocatorias. Yo era miembro del Steering Committee por 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.

Miembro del Steering Committee de Eurolatis (1999)

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

Duración: 36 meses
Institución financiadora: Unión Europea
Palabras clave: TICs y desarrollo social Sociedad de la Información
Areas de conocimiento:
Ingeniería y Tecnología / Ingeniería Eléctrica, Ingeniería Electrónica e Ingeniería de la Información / Ingeniería de Sistemas y Comunicaciones / Tecnologías de la Comunicación en Información
Eurolatis era una red entre Europa y América Latina y Caribe para el desarrollo de la Sociedad de la Información en nuestra región. La idea era organizar eventos coincidentes con los llamados en el programa marco de la Unión Europea a los efectos de presentar proyectos específicos en dichas convocatorias. Yo era miembro del Steering Committee por 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.

OTRAS PRODUCCIONES

CURSOS DE CORTA DURACIÓN DICTADOS

Análisis de algoritmos (2002)

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

EDICIÓN O REVISIÓN

Proceedings LATIN 2014 (2014)

VIOLA, A. , PARDO, A.
Anales
País: Uruguay
Idioma: Inglés
Número de páginas: 700
Areas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Teoría de la Computación

Selected papers from LATIN 2000 (2003)

VIOLA, A. , D. PANARIO , G. H. GONNET
Revista
País: Uruguay
Idioma: Inglés
Medio divulgación: Papel
Número de páginas: 350
Editorial: Elsevier
Amsterdam
Institución Promotora/Financiadora: Theoretical Computer Science (TCS)
Palabras clave: Teoría de la Computación
Areas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Teoría de la Computación

Selected papers from CLEI 2002 (2003)

VIOLA, A.
Revista

País: Uruguay
Idioma: Inglés
Medio divulgación: Internet
Web: http://www.clei.cl/cleiej/
Número de páginas: 120
Editorial: CLEI
Chile
Institución Promotora/Financiadora: Centro Latinoamericano de Informática (CLEI)
Palabras clave: Informática
Areas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Informática en general
Información adicional: Esta es una revista electrónica en donde se presentan versiones completas de los mejores trabajos aceptados en la Conferencia Latinoamericana de Informática en cada año. Yo fui presidente del Comité de Programa de CLEI 2002.

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

VIOLA, A. , D. PANARIO , G. H. GONNET
Anales
País: Uruguay
Idioma: Inglés
Medio divulgación: Papel
Número de páginas: 500
Editorial: Springer Verlag
Bonn
Institución Promotora/Financiadora: Lecture Notes in Computer Science - 1776
Palabras clave: Teoría de la Computación
Areas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Teoría de la Computación

ORGANIZACIÓN DE EVENTOS

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

BRODNIK,A , LóPEZ-ORTIZ, A. , RAMAN,V , VIOLA, A.
Congreso
Sub Tipo: Organización
Lugar: Canadá ,CANADÁ Waterloo, Ontario
Idioma: Inglés
Medio divulgación: Internet
Web: http://www.fields.utoronto.ca/programs/scientific/13-14/efficient/
Duración: 1 semanas
Palabras clave: Space Efficient Data Structures
Areas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Teoría de la Computación

Formal Methods in Security (2007)

VIOLA, A. , G. BETARTE
Otro
Lugar: Uruguay ,Montevideo Montevideo
Idioma: Español
Medio divulgación: Internet
Duración: 1 semanas
Evento itinerante: SI
Institución Promotora/Financiadora: STIC-AMSUD
Palabras clave: Information Security
Areas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Information Security
Información adicional: Tres días de seminario organizado en el marco de la red de cooperación con Francia STIC AMSUD

ITW Information Theory Workshop (2006)

VIOLA, A. , G. SEROUSSI
Concierto
Lugar: Uruguay ,Maldonado Punta del Este
Idioma: Inglés
Medio divulgación: CD-Rom
Web: http://www.fing.edu.uy/itw06
Duración: 1 semanas
Evento itinerante: SI
Catálogo: SI
Institución Promotora/Financiadora: Facultad de Ingeniería
Palabras clave: Teoría de la Información
Areas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Teoría de la Información
Información adicional: Este es el evento más importante que se haya realizado en la región en Teoría de la Información y contó con la presencia de muchos de los líderes mundiales en sus respectivas áreas de investigación. Por otro lado, tuvo el agregado de que se organizó también la reunión del Board of Governors de la ITSOC (Sociedad Internacional de la Teoría de la Información. Por otro lado, y aprovechando dicho evento, se organizó un conjunto de charlas y actividades en la la Facultad de Ingeniería con la participación de importantes investigadores dictando charlas estelares. Estas charlas estaban dirigidas a profesores y estudiantes, tanto de grado como de posgrado en Computación, Ingeniería Eléctrica y Matemáticas. Esta organización mereció la entrega de un diploma de reconocimiento oficial de parte de la IEEE en ISIT (la conferencia más prestigiosa en el mundo en el área) por la calidad mostrada en la organización del evento.

LATIN 2000 (2000)

VIOLA, A. , D. PANARIO
Congreso
Lugar: Uruguay ,Maldonado Punta del Este
Idioma: Inglés
Web: http://www.fing.edu.uy/inco/eventos/latin-2000
Duración: 1 semanas
Evento itinerante: SI
Catálogo: SI
Institución Promotora/Financiadora: Instituto de Computación
Palabras clave: Teoría de la Computación
Areas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Teoría de la Computación
Información adicional: LATIN es la conferencia más relevante a nivel mundial en Teoría de la Computación que se organiza en Latinoamérica y una de las más importantes del mundo en el área.

OTRA PRODUCCIÓN TÉCNICA

TUBA NUMBERS (2007)

VIOLA, A.

País: Estados Unidos
Idioma: Inglés
Medio divulgación: Internet
Web: http://www.research.att.com/~njas/sequences/A124453
secuencia A124453 en la The On-Line Encyclopedia of Integer Sequences de Neil Sloane
Palabras clave: linear probing hashing
Areas de 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).

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

VIOLA, A.

País: Uruguay
Idioma: Inglés
Medio divulgación: Papel
Columna cuatrimestral sobre información de eventos en Teoría de la Computación realizados en la región
Lugar: Holanda, Amsterdam
Institución Promotora/Financiadora: European Association of Theoretical Computer Science
Palabras clave: Teoría de la Computación
Areas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Teoría de la Computación
Información adicional: Esta es una columna cuatrimestral que vengo llevando desde 2001 a la fecha, en donde informo sobre las actividades más relevantes en Teoría de la Computación realizadas en la región.

Evaluaciones

EVALUACIÓN DE PROYECTOS

EVALUACIÓN INDEPENDIENTE DE PROYECTOS

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

Uruguay
Presidente de concurso de tesis de Maestría CLEI - UNESCO
Cantidad: Mas de 20
A partir de 2009, voy a ser presidente del concurso de tesis de Maestría CLEI - UNESCO.

Universidad de San Luis (2008 / 2008)

Argentina
Universidad de San Luis
Cantidad: Menos de 5
Evaluador externo de la propuesta de tesis de doctorado de Nora Reyes.

PDT - ANII (2006 / 2008)

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

Conicet (2005 / 2008)

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

cooperación internacional México - Argentina (2005 / 2008)

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

ECOS - cooperación Argentina - Francia (2004 / 2008)

Francia
ECOS - cooperación Argentina - Francia
Cantidad: Menos de 5

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

CLEI - UNESCO (1996 / 2008)

Uruguay
CLEI - UNESCO
Cantidad: Mas de 20
Desde 1996 he participado en varios tribunales del concurso Latinoamericano de Tesis de Maestría en Informática financiado conjuntamente por el CLEI (Centro 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 PUBLICACIONES

COMITÉ EDITORIAL

ACM Transactions on Algorithms (2009 / 2013)

Cantidad: Menos de 5

Combinatorics, Probability and Computing (2008 / 2013)

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

RAIRO (2005 / 2010)

Cantidad: Menos de 5
Revista francesa de informática teórica

IEEE Transactions on Information Theory (2002 / 2013)

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

Random Structures and Algorithms (1998 / 2013)

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

Algorithmica (1998 / 2010)

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

Theoretical Computer Science (1996 / 2013)

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

EVALUACIÓN DE EVENTOS Y CONGRESOS

XII Latin-American Algorithms, Graphs and Optimization Symposium (LAGOS 2023) (2023)

Comité programa congreso
México
Arbitrado

LATINCRYPT 2023 (2023)

Comité programa congreso

Ecuador
Arbitrado

15th Latin American Theoretical Informatics Symposium (LATIN 2022) (2022)

Comité programa congreso
México
Arbitrado

Symposium on the Foundations of Responsible Computing (FORC 2022) (2022)

Comité programa congreso
Estados Unidos
Arbitrado

Universidad de Harvard
Es la conferencia más importante del mundo en esta área.

XI Latin and American Algorithms, Graphs and Optimization Symposium (LAGOS 2021) (2021)

Comité programa congreso
Brasil
Arbitrado

Fui seleccionado como uno de los 3 miembros del Comité de Programa para elegir el "Best Paper Award" de la conferencia.

LATINCRYPT 2021 (2021)

Comité programa congreso
Colombia
Arbitrado

37th Symposium on Theoretical Aspects of Computer Science (STACS 2020) (2020)

Comité programa congreso
Francia

STACS2020 (2019 / 2019)

Comité programa congreso
Francia
Arbitrado

Una de las conferencias más importante en Teoría de la Computación de Europa.

STACS2020 (2019 / 2019)

Comité programa congreso
Francia
Arbitrado

Una de las conferencias más importante en Teoría de la Computación de Europa.

LATINCRYPT 2019 (2019 / 2019)

Comité programa congreso
Chile
Arbitrado

LATINCRYPT 2017 (2017)

Comité programa congreso
Cuba
Arbitrado

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

ANALCO 2018 (2017)

Comité programa congreso
Estados Unidos
Arbitrado

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

Brasil

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

India

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

Comité programa congreso
Argentina

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

ALEA 2015 (co-organizador) (2014)

Francia

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

LATINCRYPT 2014 (2014)

Brasil

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

Comité programa congreso
Brasil

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

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

Uruguay

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

Canadá

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

Canadá

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

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

India

LATINCRYPT 2012 (2011)

Chile

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

Comité programa congreso
Brasil

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

LATIN 2012 (2011)

Perú

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

LATINCRYPT 2010 (2010)

México

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

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

India

Conference Proceedings publicados por la IEEE Computer Society Conference Publishing Services

LATIN 2010 (Latin American Theoretical INformatics) (2009)

México

Miembro del Comité de Programa

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

Uruguay

Miembro del Comité de Programa

Sistema nacional de investigador (2009)

Uruguay

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

ANALCO 2008 (Analytic Algorithms and Combinatorics) (2008)

Estados Unidos

Miembro de Comité de Programa Organizado por la SIAM

LATIN 2008 (Latin American Theoretical INformatics) (2008)

Brasil

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

Sistema Nacional de Investigador (2008)

Uruguay

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

LAGOS/GRACO 2009 (2008)

Brasil

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

CLEI 2007 (Conferencia Latinoamericana de Informática) (2007)

Costa Rica

Miembro de Comité de Programa

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

Francia

Miembro de Comité de Programa

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

Argentina

Miembro de Comité de Programa

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

Chile

Miembro de Comité de Programa

LATIN 2006 (2006)

Chile

Miembro de Comité de Programa

IEEE Information Theory Workshop (ITW06) (2006)

Uruguay

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

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

Chile

Miembro de Comité de Programa

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

Colombia

Miembro de Comité de Programa

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

México

Miembro de Comité de Programa

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

España

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

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

México

Miembro del Comité de Programa

CLEI 2003 (Conferencia Latinoamericana de Informatica) (2003)

Bolivia

Miembro del Comité de Programa

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

Bolivia

Miembro del Comité de Programa

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

Argentina

Miembro del Comité de Programa

CLEI 2002 (Conferencia Latinoamericana de Informatica) (2002)

Uruguay

Presidente del Comité de Programa

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

Canadá

Miembro del Comité de Programa

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

Costa Rica

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

LATIN 2000 (Latin American Theoretical INformatics) (2000)

Uruguay

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

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

Argentina

Miembro del Comité de Programa

EVALUACIÓN DE PREMIOS

Premios Anuales de Literatura (2010 / 2010)

Uruguay

Cantidad: Menos de 5
Ministerio de Educación y Cultura
categoría: OBRAS SOBRE INVESTIGACIÓN Y DIFUSIÓN CIENTÍFICA.

EVALUACIÓN DE CONVOCATORIAS CONCURSABLES

ANII - diferentes convocatorias (2010 / 2013)

Uruguay
Cantidad: Mas de 20
ANII
Varias evaluaciones realizadas para diversos programas de ANII ya sea como miembro de comite de programa o como evaluador.

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

Argentina
Cantidad: De 5 a 20
CONEAU
Evaluador extranjero en el proceso de acreditación de carreras de Computación en Argentina.

Proyectos de Iniciación a la Investigación Científica (2009)

Uruguay
Cantidad: De 5 a 20
CSIC - UDELAR
Participación en la comisión de evaluación

FCE (2008)

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

PDT (2006)

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

JURADO DE TESIS

Doctorado en informática (2022)

Jurado de mesa de evaluación de tesis
Sector Extranjero/Internacional/Otros / École normale supérieure (Paris) / ENS Paris , Francia
Nivel de formación: Doctorado
Estuve en el tribunal de tesis de doctorado de Octavio Perez-Kempner sobre ""Malleable Cryptography: Advances and Applications to Privacy-enhancing Technologies".

Doctorado en Computación (2016)

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

Tesis de doctorado de Nicolás Rollin.

Doctorado en Computación (2015 / 2016)

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

Doctorado en Informática (2009)

Jurado de mesa de evaluación de tesis
Sector Extranjero/Internacional/Otros / Universite de Caen / GREYC , Francia
Nivel de formación: Doctorado
Participación en el tribunal de tesis de doctorado de Antonio Vera. Fui uno de los dos miembros que tuvo que hacer el informe oficial de experto.

Formación de RRHH

TUTORÍAS CONCLUIDAS

POSGRADO

Monedas digitales de bancos centrales (2018 - 2020)

Tesis de maestria
Sector Educación Superior/Público / Universidad de la República / Facultad de Ingeniería , Uruguay
Programa: Maestría en Gestión de la Innovación
Tipo de orientación: Tutor único o principal
Nombre del orientado: Grabriel Yermán
País: Uruguay

Ańalisis Dinámico en Combinatoria de Palabras

Tesis de doctorado
Sector Educación Superior/Público / Facultad de Ingeniería , Francia
Programa: Doctorado en Informática (UDELAR-PEDECIBA)
Tipo de orientación: Cotutor en pie de igualdad
Nombre del orientado: Pablo Rotondo
País: Francia
Palabras Clave: Análisis dinámico de algoritmos
Areas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación
Doctorado en cotutela con la Universidad de Paris 7. La orientadora del lado francés es Valérie Berthé, contando con la activa participación de Brigitte Vallée de la Universidad de Caen.

Combinatoria Analítica y Aplicaciones

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

Seguridad en redes GSM

Tesis de maestria
Sector Educación Superior/Público / Universidad de la República / Facultad de Ingeniería , Uruguay
Programa: Maestría en Ingeniería (Ingeniería Eléctrica)
Nombre del orientado: Eduardo Cota
País: Uruguay
Palabras Clave: Redes GSM Seguridad

Areas de conocimiento:
Ingeniería y Tecnología / Ingeniería Eléctrica, Ingeniería Electrónica e Ingeniería de la Información / Telecomunicaciones / Seguridad en Redes GSM
Co-dirección de tesis junto con Eduardo Giménez. El supervisor de estudios es Pablo Belzarena.

Tree models: Algorithms and Information Theoretic Properties

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

Análisis del algoritmo de compresión PPM

Tesis de maestria
Sector Educación Superior/Público / Universidad de la República / Facultad de Ingeniería , Uruguay
Programa: Maestría en Informática (UDELAR-PEDECIBA)
Nombre del orientado: Jorge Merlino
País: Uruguay
Palabras Clave: Algoritmo PPM
Areas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Teoría de la Información
Supervisor de esutdios y co-orientador de tesis junto con Marcelo Weinberger (HP Labs, California)

Implementacion eficiente de modelos de markov dispersos usando algoritmos genéticos

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

Texture Mixing via Universal Simulation

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

GRADO

IOTA: Alternativa a blockchain (2022 - 2023)

Tesis/Monografía de grado
Sector Educación Superior/Público / Universidad de la República / Facultad de Ingeniería / Instituto de Computación , Uruguay
Programa: Licenciatura en Computación
Tipo de orientación: Tutor único o principal

Nombre del orientado: Martín Rivadavia
País: Uruguay

Test de primalidad y algoritmos de factorización en criptografía: aspectos matemáticos y computacionales (2021 - 2022)

Tesis/Monografía de grado
Sector Educación Superior/Público / Universidad de la República / Facultad de Ciencias / Centro de Matemáticas , Uruguay
Programa: Licenciatura en Matemática
Tipo de orientación: Cotutor en pie de igualdad (VIOLA, A. , C. Qureshi)
Nombre del orientado: Bruno Hernández
País: Uruguay
Trabajo para doble titulación Ingeniería en Computación y Licenciatura en Matemática. Por motivo de fechas y de tribunal realizó dos defensas, una en Computación y otra en matemáticas. Los documentos fueron diferentes en el sentido de que en el documento de computación se hizo énfasis en los aspectos algorítmicos del problema mientras que en el documento de matemática se hizo énfasis en los aspectos matemáticos del mismo.

Aplicaciones de computación cuántica a la inteligencia artificial (2020 - 2022)

Tesis/Monografía de grado
Sector Educación Superior/Público / Universidad de la República / Facultad de Ingeniería / Instituto de Computación , Uruguay
Programa: In geniería en Computación
Tipo de orientación: Cotutor (VIOLA, A. , SERGIO NESMACHNOW)
Nombre del orientado: Cobelli, Nicolás Juambeltz, Nelson Pérez, Javier Techera, Melisa
País: Uruguay

Test de primalidad y algoritmos de factorización en criptografía: aspectos matemáticos y computacionales (2021 - 2021)

Tesis/Monografía de grado
Sector Educación Superior/Público / Universidad de la República / Facultad de Ingeniería / Instituto de Computación , Uruguay
Programa: In geniería en Computación
Tipo de orientación: Cotutor en pie de igualdad (VIOLA, A. , C. Qureshi)
Nombre del orientado: Bruno Hernández
País: Uruguay
Trabajo para doble titulación Ingeniería en Computación y Licenciatura en Matemática. Por motivo de fechas y de tribunal realizó dos defensas, una en Computación y otra en matemáticas. Los documentos fueron diferentes en el sentido de que en el documento de computación se hizo énfasis en los aspectos algorítmicos del problema mientras que en el documento de matemática se hizo énfasis en los aspectos matemáticos del mismo.

Manejo de la privacidad en permissioned blockchain (2020 - 2021)

Tesis/Monografía de grado
Sector Educación Superior/Público / Universidad de la República / Facultad de Ingeniería / Instituto de Computación , Uruguay
Programa: Ingenieria en Computacion
Tipo de orientación: Cotutor en pie de igualdad (VIOLA, A. , Octavio Perez-Kempner)
Nombre del orientado: Matías Leal y Maximiliano Montiglio
País: Uruguay
Palabras Clave: zero knowledge blockchain privacidad
Areas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación e Información / criptografía, seguridad, comunicaciones.
El cotutor es Octavio Perez-Kempner quien está realizando su doctorado en temas relacionados con la monografía en ENS Paris.

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

Tesis/Monografía de grado
Sector Educación Superior/Público / Universidad de la República / Facultad de Ingeniería , Uruguay
Programa: Licenciatura en Computación
Tipo de orientación: Tutor único o principal
Nombre del orientado: Francisco Castro

País: Uruguay
Palabras Clave: ataque AES
Areas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Funciones Booleanas
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / criptografia

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

Tesis/Monografía de grado
Sector Educación Superior/Público / Universidad de la República / Facultad de Ingeniería , Uruguay
Programa: Ingeniería en Computación
Tipo de orientación: Tutor único o principal
Nombre del orientado: Sebastián Fonseca / María Cecilia García
País: Uruguay
Areas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / criptografia

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

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

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

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

Generaciòn aleatoria eficiente de funciones booleanas resilientes

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

Predicción de Estructura Secundaria de Proteínas

Tesis/Monografía de grado
Sector Educación Superior/Público / Universidad de la República / Facultad de Ingeniería , Uruguay
Programa: Ingeniería en Computación
Nombre del orientado: Elisa Budelli

País: Uruguay
Palabras Clave: prediccion de estructura secundaria de proteinas
Areas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / bioinformática
Trabajo co-dirigido con Fernando Alvarez de la Facultad de Ciencias

Algoritmos óptimos de compresión

Tesis/Monografía de grado
Sector Educación Superior/Público / Universidad de la República / Facultad de Ingeniería , Uruguay
Programa: Ingeniería en Computación
Nombre del orientado: Florencia da Silveira: Karina Alvarez
País: Uruguay
Palabras Clave: Algoritmo Context
Areas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Teoría de la Información
Co-dirigido con Alvaro Martín

Corrección de errores para distribución de datos en redes

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

Codigos de paridad de baja densidad

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

El comercio electrónico y los sistemas de pago online

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

Simulación de un mercado de transacciones financieras por internet

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

Computación / criptografia

Inserción de marcas de tiempo en certificados digitales

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

Criptografía para dispositivos de bajos recursos

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

Estudio de Transacciones electrónicas en internet

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

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

Tesis/Monografía de grado
Sector Educación Superior/Público / Universidad de la República / Facultad de Ingeniería , Uruguay
Programa: Ingeniería en Computación
Nombre del orientado: Leonardo Dominguez; Cecilia Fernández
País: Uruguay
Palabras Clave: comercio electrónico
Areas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / criptografia

Sistema de comercio electrónico

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

Inserción de marcas de agua en imágenes digitales

Tesis/Monografía de grado
Sector Educación Superior/Público / Universidad de la República / Facultad de Ingeniería , Uruguay
Programa: Ingeniería en Computación
Nombre del orientado: Fabian Martínez; Gabriela Delfino

País: Uruguay
Palabras Clave: watermarking
Areas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / criptografia

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

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

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

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

Buscador Académico Uruguayo

Tesis/Monografía de grado
Sector Educación Superior/Público / Universidad de la República / Facultad de Ingeniería , Uruguay
Programa: Ingeniería en Computación
Nombre del orientado: Alfredo Espasandin; Ricardo Martínez
País: Uruguay
Palabras Clave: recuperación de información
Areas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Sistemas de Información

OTRAS

Criptografía post-cuántica basada en látices

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

Relevamiento de técnicas de clusterización de identidades en criptomonedas

Otras tutorías/orientaciones
Sector Educación Superior/Público / Universidad de la República / Facultad de Ingeniería , Uruguay
Tipo de orientación: Cotutor en pie de igualdad
Nombre del orientado: Alex Rostan, Fabricio Garin,Lucas Bouissa
País: Uruguay
Palabras Clave: blockchain monedas digitales
Areas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la

Computación e Información / criptografía
Proyecto de grado en co-dirección con Germán Ferrari

Relevamiento de ataques de seguridad a las redes de Bitcoin y Ethereum

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

Funciones Booleanas inmunes a la correlación.

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

TUTORÍAS EN MARCHA

POSGRADO

Formal and experimental methods for measuring bias in datasets (título tentativo) (2021)

Tesis de doctorado
Sector Extranjero/Internacional/Otros / Northeastern University / Khoury College of Computer Sciences , Estados Unidos
Programa: Ph.D. in Computer Science
Tipo de orientación: Cotutor en pie de igualdad (VIOLA, A. , BAEZA-YATES,R.)
Nombre del orientado: Bruno Scarone
País/Idioma: Estados Unidos,
Bruno Scarone está realizando sus estudios de doctorado en Northeastern University en el área de Ciencias de Datos e Inteligencia Artificial. Como todavía no tiene aún completamente definida su tesis, puse un nombre tentativo de acuerdo a sus avances actuales. Su orientador formal es Ricardo Baeza-Yates científico extremadamente reconocido a nivel internacional en el área. El área está en etapas primitivas de desarrollo y en general los resultados son fundamentalmente experimentales. Dado que Bruno tiene interés es realizar aportes formales en estos temas integrando modelos teóricos con resultados experimentales, yo me integré en la codirección (con el apoyo de Ricardo Baeza-Yates) para guiar los aspectos de modelado matemáticos de la tesis. No tengo una posición formal de codirector de tesis dado que no pertenezco a la Northeastern University pero estoy realizando la cosupervisión de hecho. Luego de consultarle explícitamente, Ricardo Baeza-Yates me autorizó a que me presente como cotutor en pie de igualdad en este CVUy.

Desencriptado de mensaje del MLN codificado en la tapa del libro EVA en los años '80. (2019)

Tesis de maestria
Sector Educación Superior/Público / Universidad de la República / Facultad de Ingeniería , Uruguay
Tipo de orientación: Cotutor en pie de igualdad
Nombre del orientado: Francisco Castro
País/Idioma: Uruguay, Español
Palabras Clave: criptografía mensaje MLN exterior
Areas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación e Información / criptografía
Es una tesis codirigida con Joachim von zur Gathen (Universidad de Bonn). El tema es el desencriptado de un mensaje mandado por miembros del MLN en Suecia al Penal de Libertad a principio de los años '80 codificado en la tapa de un libro llamado EVA. Hay una publicación

aceptada al respecto en colaboración también con Juan José Cabezas y Jorge Tiscornia.

Otros datos relevantes

PREMIOS, HONORES Y TÍTULOS

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

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

Sistema Nacional de Investigador (Nivel II) (2009)

ANII

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

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

Autor de la secuencia TUBA NUMBERS (2007)

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

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

DICyT

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

Capman & Hall/CRC

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

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

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

Dagstuhl Seminars

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

Wiley-Interscience

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

AofA

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

DICyT

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

CRC-PRESS

Citado en "The Art of Computer Programming: Volume 3:" de Donald E. Knuth, una de las mejores 12 monografías físico-matemáticas del siglo XX (1997)

(Internacional)
https://www-cs-faculty.stanford.edu/~knuth/taocp.html
Uno de los trabajos citados es realizado en colaboración directa con Donald Knuth (autor de la monografía) en el problema que dio origen a esta colección de libros. Es considerada una de las 12 mejores monografías físico-matemáticas del siglo XX por presentar las bases matemáticas de la Ciencia de la Computación.

International Student Fee Waiver (1990)

Universidad de Waterloo

Student Fellowship (1989)

NSERC - Canadá

BECA PEDECIBA para realizar posgrado en Canadá (1987)

Pedeciba

PRESENTACIONES EN EVENTOS

Philippe Flajolet and Analytic Combinatorics (2011)

Simposio
Philippe Flajolet and his theoretical contributions in the analysis of hashing algorithms
Francia
Tipo de participación: Conferencista invitado
Nombre de la institución promotora: INRIA Palabras Clave: Hashing Algorithms
Areas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / combinatoria analítica
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / analisis de algoritmos
Es un evento especial organizado en honor a Philippe Flajolet,, líder de nuestra área de investigación, miembro de la Academia de Ciencias de Francia y quien falleció en marzo 2011.

Escuela de Criptografia SP-ASCrypto (2011)

Simposio
Boolean Functions in cryptography

Brasil
Tipo de participación: Conferencista invitado
Nombre de la institución promotora: CNPQ Palabras Clave: funciones booleanas
Areas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / 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.

Invitacion a participar en el seminario del laboratorio (2010)

Seminario
Distributional analisis of the parking problem and the Robin Hood Linear probing algorithm with buckets
Francia
Tipo de participación: Expositor oral
Nombre de la institución promotora: Ecole Polytechnique Palabras Clave: hashing parking problem with buckets linear probing with buckets Tuba Numbers
Areas de conocimiento:
Ciencias Naturales y Exactas / Matemáticas / Matemática Aplicada / Analisis de algorithmos y combinatoria
Invitacion a realizar trabajos de investigacion conjunta y presentacion de mis resultados recientes de investigacion.

(2009)

Simposio
Some asyptotic issues related with the exact distribution of Individual Displacements in Linear Probing Hashing
Canadá
Tipo de participación: Palabras Clave: linear probing hashing
Areas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / analisis de algoritmos

Dagstuhl Seminar on Data Structures (2008)

Seminario
Efficient Data Structures for Universal Denoising
Alemania
Tipo de participación: Expositor oral
Carga horaria: 30
Nombre de la institución promotora: Schloss Dagstuhl - Leibniz Center for Informatics Los seminarios Dagstuhl, son eventos en los que se participa sólo por invitación. Un grupo de líderes mundiales en un área temática organiza uno de estos seminarios y realiza invitación a expertos y estudiantes de doctorado en dichas áreas para realizar 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.

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

Encuentro
INFORMATION TECHNOLOGIES TO THE HELP OF CITIZEN PARTICIPATION IN PUBLIC DECISIONS AND PUBLIC EDUCATION
Argentina
Tipo de participación: Expositor oral

Nombre de la institución promotora: CLEI y SBC (Sociedad Brasilera de Computación) Palabras Clave: participación ciudadana tecnologías de la información y educación decisiones públicas
Areas de conocimiento:
Ingeniería y Tecnología / Ingeniería Eléctrica, Ingeniería Electrónica e Ingeniería de la Información / Ingeniería de Sistemas y Comunicaciones / Sociedad de la Información y Conocimiento
En este evento, que contó también con la participación de Microsoft (auspiciante de la iniciativa LACCIR) se discutieron sobre diversas iniciativas orientadas a pensar grandes áreas temáticas de investigación y desarrollo vinculadas a la computación y sus usos sociales, a los efectos de generar un movimiento regional de apoyo al financiamiento de dichas actividades de alto impacto en el desarrollo de la región. Mi actividad consistió en presentar la exposición que comento, participar en los grupos de trabajos formados en dicho evento, y participar en la elaboración de un documento final.

Workshop on Information Theory and Applications (2007)

Simposio
Combinatorial characterization of Resilient Functions
Estados Unidos
Tipo de participación: Expositor oral
Nombre de la institución promotora: Universidad de San Diego Es un evento por invitación y es uno de los eventos más importantes y relevantes en Teoría de la Información.

11th seminar on Analysis of Algorithms (2006)

Seminario
Optimal prefix codes for pairs of geometrically-distributed random variables
Bélgica
Tipo de participación: Expositor oral
Nombre de la institución promotora: Alden Biesen Este es un evento por invitación organizado por la comunidad internacional de Analisis de Algoritmos (a la cual pertenezco activamente) y es la continuación de los seminarios Dagstuhl en el área.

10th Seminar on Analysis of Algorithms (2004)

Seminario
Adaptive Sampling Strategies for Quickselect
Estados Unidos
Tipo de participación: Expositor oral
Nombre de la institución promotora: MSRI Este es un evento por invitación organizado por la comunidad internacional de Analisis de Algoritmos (a la cual pertenezco activamente) y es la continuación de los seminarios Dagstuhl en el área.

9th Seminar on Analysis of Algorithms (2003)

Seminario
On worst case Robin Hood Hashing
Italia
Tipo de participación: Expositor oral
Nombre de la institución promotora: Universidad de Florencia Este es un evento por invitación organizado por la comunidad internacional de Analisis de Algoritmos (a la cual pertenezco activamente) y es la continuación de los seminarios Dagstuhl en el área.

Workshop on Combinatorics, Algorithms and Applications (2003)

Simposio
Adaptive Sampling Strategies for Quickselect
Brasil
Tipo de participación: Conferencista invitado
Nombre de la institución promotora: Universidad de San Pablo

8th Seminar on Analysis of Algorithms (2002)

Seminario
Exact distribution of individual displacements in linear probing hashing
Austria
Tipo de participación: Expositor oral
Nombre de la institución promotora: Universidad de Viena Este es un evento por invitación organizado por la comunidad internacional de Analisis de Algoritmos (a la cual pertenezco activamente) y es la continuación de los seminarios Dagstuhl en el área.

KnuthFest (2002)

Encuentro
KnuthFest
Estados Unidos
Tipo de participación: Otros
Nombre de la institución promotora: Universidad de Stanford KnuthFest fue un evento de celebración de los 64 años de D. E. Knuth. El Dr. Knuth es la persona más relevante de la segunda mitad del siglo XX en Computación. Es el autor de la famosa colección de libros "The Art of Computer Programming", que es la colección de libros más vendida y de mayor impacto en la historia de la computación. Por otro lado es el creador del área de Análisis de Algoritmos, una de mis principales áreas de investigación. Este fue un evento realizado por invitación, en donde sólo 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".

7th Seminar on Analysis of Algorithms (2001)

Seminario
Analysis of Rabin`s Irreducibility Test for Polynomials over Finite Fields
Francia
Tipo de participación: Conferencista invitado
Nombre de la institución promotora: Universidad de Caen Este es un evento por invitación organizado por la comunidad internacional de Analisis de Algoritmos (a la cual pertenezco activamente) y es la continuación de los seminarios Dagstuhl en el área. En esta ocasión fui invitado a dar una charla estelar de 1 hora de duración.

Montreal - Ottawa Analysis of Algorithms Workshop (2001)

Simposio
The Effect of Deletions on Different Insertion Disciplines for Hash Tables
Canadá
Tipo de participación: Conferencista invitado
Nombre de la institución promotora: Universidad de Carleton

6th Seminar on Analysis of Algorithms (2000)

Seminario
Open problems related with Linear Probing Hashing with Buckets
Polonia
Tipo de participación: Expositor oral
Nombre de la institución promotora: Universidad de Gdansk Este es un evento por invitación organizado por la comunidad internacional de Analisis de Algoritmos (a la cual pertenezco activamente) y es la continuación de los seminarios Dagstuhl en el área.

Encuentro Brasilero de Combinatoria (2000)

Encuentro
The symbolic method in combinatorics
Brasil
Tipo de participación: Conferencista invitado
Nombre de la institución promotora: Universidad de San Pablo

5th Seminar on Analysis of Algorithms (1999)

Seminario
The Effect of Deletions on Different Insertion Disciplines for Hash Tables
España
Tipo de participación: Expositor oral
Nombre de la institución promotora: Universidad Politécnica de Catalunya Este es un evento por invitación organizado por la comunidad internacional de Analisis de Algoritmos (a la cual pertenezco activamente) y es la continuación de los seminarios Dagstuhl en el área.

Dagstuhl Seminar on Data Structures (1997)

Seminario
Analysis of the total displacement in a linear probing hash table.
Alemania
Tipo de participación: Expositor oral
Nombre de la institución promotora: Schloss Dagstuhl - Leibniz Center for Informatics Los

seminarios Dagstuhl, son eventos en los que se participa sólo por invitación. Un grupo de líderes mundiales en un área temática organiza uno de estos seminarios y realiza invitación a expertos y estudiantes de doctorado en dichas áreas para realizar 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.

DIMACS Seminar on Probabilistic Analysis of Algorithms (1997)

Seminario
The analysis of linear probing hashing with buckets
Estados Unidos
Tipo de participación: Expositor oral
Nombre de la institución promotora: DIMACS Este es un evento por invitación organizado por la comunidad internacional de Analisis de Algoritmos (a la cual pertenezco activamente) y es la continuación de los seminarios Dagstuhl en el área.

Dagstuhl Seminar on Analysis of Algorithms (1995)

Seminario
The diagonal Poisson transform and its application to the analysis of a hashing scheme
Alemania
Tipo de participación: Expositor oral
Nombre de la institución promotora: Schloss Dagstuhl - Leibniz Center for Informatics Los seminarios Dagstuhl, son eventos en los que se participa sólo por invitación. Un grupo de líderes mundiales en un área temática organiza uno de estos seminarios y realiza invitación a expertos y estudiantes de doctorado en dichas áreas para realizar 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.

JURADO/INTEGRANTE DE COMISIONES EVALUADORAS DE TRABAJOS ACADÉMICOS

"Malleable Cryptography: Advances and Applications to Privacy-enhancing Technologies". (2022)

Candidato: Octavio Perez-Kempner
Tipo Jurado: Tesis de Doctorado
VIOLA, A. , Olivier Blazy , Sébastien Canard , Jean-Sébastien Coron , Anna Lysyanskaya , Carla Ràfols , Daniel Slamanig , Pascal Lafourcade , David Naccache , David Manset
Doctorado en computación / Sector Extranjero/Internacional/Otros / Institución Extranjera / École normale supérieure (Paris) / Francia
Sitio Web: https://www.octavio.pk/soutenance.html
País: Francia
Idioma: Inglés
Tribunal de primer nivel de expertos. Por ejemplo Anna Lysyanskaya era la presidenta del momento de la International Association for Cryptologic Research (IACR) la asociación de criptología más importante del mundo.

De l?usage des op ?erateurs en combinatoire : construction, analyse et g ?en ?eration al ?eatoire. (2016)

Candidato: Nicolas Rolin
Tipo Jurado: Tesis de Doctorado

VIOLA, A. , Olivier BODINI , Antoine GENITRIN , ulien CLEMENT , Fr ?ed ?erique BASSINO , Cyril NICAUD , Vlady RAVELOMANANA
HDR / Sector Extranjero/Internacional/Otros / Institución Extranjera / Université de Paris Nord XIII / Francia
País: Francia
Idioma: Francés
He sido citado como uno de los dos revisores oficiales expertos de la tesis.

Metadata-based Provenance (2015)

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

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

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

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

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

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

Candidato: Varios Candidatos
Tipo Jurado: Otras
GORDILLO, S , JOFRE, A , VIOLA, A.
Ingeniería / Sector Extranjero/Internacional/Otros / Institución Extranjera / Universidad de Buenos Aires / Argentina
País: Argentina
Idioma: Español
Palabras Clave: Profesor Regular Asociado
Areas de conocimiento:
Ciencias Naturales y Exactas / Ciencias de la Computación e Información / Ciencias de la Computación / Ingeniería de Software
NO encontré otro lugar en el CVuy para poner este tipo de evaluación

(2008)

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

(2005)

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

(2004)

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

(2004)

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

(2003)

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

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.

He sido miembro del Consejo de Facultad por el orden docente de 2004 a 2013, he sido varias veces miembro del Claustro de Facultad, he sido miembro suplente de la Comisión de Instituto de computación de la Facultad de Ingeniería de 2014 a 2018 y miembro de la Comisión de Planes de Estudio del Claustro de 2014 a 2017.

Estoy trabajando profundamente en colaboración con centros internacionales de gran reconocimiento. Si se la actuación profesional, tengo amplia colaboración con Francia, España, Alemania, Canadá, Chile, Brasil y Argentina entre otros países. Parte fundamental es la generación de redes internacionales como STIC-AMSUD (tengo varios proyectos financiados en este marco) y con la creciente participación de estudiantes uruguayos. También he colaborado profundamente en la creación del IFUMI (Laboratorio Internacional

Integrado entre CNRS y la Universidad de la República, donde participo en el área que vincula la matemática e informática - "MATH-INFO"), y participo de otro laboratorio similar con Argentina llamado SINFIN.

Pablo Rotondo defendió su tesis de doctorado en cotutela con Paris VII en 2018, siendo los codirectorres científicos Valérie Berthé (Paris VII), Brigitte Vallée (Caen) y Alfredo Viola (Uruguay).

Varios estudiantes están participando en proyectos o tesis de posgrado en el marco de la colaboración internacional. En estos momentos un miembro del grupo (Octavio Perez-Kempner) está haciendo su doctorado en Francia y colabora en dirección de proyecto de grado sobre "manejo de la privacidad en blockchain" desde allá. Por otro lado Francisco Castro está haciendo la Maestría en Informática en codirección entre Joachim von zur Gathen (Alemania) y Alfredo Viola (Uruguay). Su tesis se basa en el desencriptado de un mensaje codificado por miembros del MLN en el exilio a comienzo de los años '80 en la tapa de un libro llamado EVA y enviado al Penal de Libertad. Presentamos el trabajo en la conferencia internacional más importante vinculada a Historia de la Criptografía (HISTOCRYPT 2019) y el trabajo es en colaboración con Jorge Tiscornia (quien nos presentó todo el problema a resolver) y Juan José Cabezas (Instituto de Computación).

En estos momentos tengo 4 grados 1, 20 hs. financiado por un proyecto CSIC trabajando en un tema de profunda actualidad como lo es el de la Criptografía Poscuántica. En 2017 el NIST lanzó un llamado mundial para presentar nuevos estándares criptográficos que sean resistentes a ataques cuánticos. Conozco personalmente varias personas que presentaron propuestas basados en problemas vinculados con reticulados. Estudiar rigurosamente estas propuestas (tratando de encontrar modelos matemáticos que puedan acotar probabilidades de falla, vinculadas con diversos tipos de ataques prácticos) es un trabajo extremadamente difícil. Por otro lado, el grupo de investigación de la Universidad de Caen (Francia) es experto en el estudio de problemas sobre reticulados. Por este motivo, dado que el llamado NIST aún está en proceso de evaluación (que lleva varios años) hay cuatro estudiantes de grado (dos de ellos estudiando también la Licenciatura en Matemáticas de la Facultad de Ciencia) estudiando estas propuestas, tratando de ver cómo podríamos colaborar con nuestros análisis.

Es importante recalcar que este proyecto NIST puede estar muy lejos de la capacidad de propuestas claras y prácticas, pero el resultado va a tener la gran virtud de que se enfrentan con problemas muy difíciles, donde van a aprender mucha matemática y mucha criptografía, y van a tener contacto con mucha gente experta a niel internacional, con lo cual luego se pueden hacer doctorados en colaboración conjunta en temas de fundamental importancia actual.

Por otro lado, he tenido la visita de muchos investigadores muy prestigiosos (como parte de intercambios internacionales de investigación científica) quienes no sólo han realizado proyectos de investigación conjunta con la participación estudiantil uruguaya, sino que además han dado cursos muy importantes de grado y posgrado, y con mucho éxito.

La "construcción institucional" consiste en adaptarnos (y aprovechar!) los grandes cambios en la Historia de la Humanidad (en un mundo global integrado por las TICs), en donde está profundamente en duda cuál es el rol de las Uniersidades en este contexto, y cómo va a ser la generación y difusión del conocimiento en este contexto.

Estamos profundamente convencidos de que el camino pasa por la craeación de muchos "Laboratorios Internacionales Integrados" con la participación de docentes y estudiantes de los más diversos lugares del mundo (incluyendo de Uruguay!) y en colaboración conjunta, dinámica, usando las TICs, y aprovechando momentos de encuentro presencial (muchos de ellos en Uruguay). En el medio hay cursos dictados en conjunto, proyectos de grado y tesis de posgrado dirigidos en conjunto (por medio de las TICs y visitas presenciales), y "formación de futuro" en temas de fundamental importancia (como los de "Criptografía Poscuántica") con la participación de líderes internacionales. Consideramos que es el camino a seguir, y que es la forma moderna de hacer "construcción institucional" y que además es bien sólida, y con bases para ir generando un fuutro muy exitoso y esperanzador. Así es nuestra experiencia, y así es el camino que hemos seguido (aún en la enfermedad GRAVE como la que tengo, dado que estos vínculos son muy fuertes y los estudiantes pueden seguir adelante a pesar de mis difucultades originadas por esta enfermerdad).

Otra actividad de construcción institucional importante (en el sentido de que trata de impulsar la investigación científica no sólo en Uruguay sino en toda la región) ha sido la creación y apoyo de conferencias internacionales de gran impacto y visibilidad.
En este sentido, he sido cofundador de dos conferencias LANC y LATINCRYPT.
LANC la fundamos en 2001, y estuve colaborando hasta el 2005 en el cual nunca más fui solicitado para colaborar en el PC, cuando tomó el poder un docente quien la acomodó "a su gusto". A partir de ese momento nunca más (no precisamente por voluntad propia!) fui llamado a colaborar.
LATINCRYPT la fundamos en 2010 como producto de un proyecto STIC-AMSUD relacionado con criptografía (FMCRYPTO) y de la cual soy miembro del Steering Committe. No sólo hemos fomentado una conferencia que se va estabilizando cada más a nivel internacional, sino que asociado a las conferencias realizamos escuelas con la participación de varios de los investigadores mas importantes que participan en los eventos. Es importante recalcar que este año (2019) participaron 6 estudiantes de Uruguay, y que en

cada edición hay más participación nacional.
LATIN es la conferencia en Teoría de la Computación más importante que se realiza en la región. Yo la organicé dos veces en Uruguay, y en 2014 fui presidente del comité de programa (mientras Alberto Pardo fue el presidente del comité de organización). En estos momentos soy miembro del SC, y estamos trabajando muy fuertemente para apoyar el desarrollo de la Informática Teórica en la región (incluyendo en nuestro país).
Un último punto fundamental es que Pierrick Mèaux de Francia viene a realizar un posdoctorado en Marzo 2020 a Uruguay a trabajar conmigo. Vamos a trabajar en diversos problemas relacionados con el uso de funciones Booleanas en Criptografía y en Criptografía Homomórfica (un área relatiamente nueva y con mucho impacto tanto teórico como práctico). Para mi es un gran honor recibir a estudiantes del primer mundo trabajando con investigadores radicados en el Uruguay. Es una muestra de que no sólo "se va en una dirección", sino que también los estudiantes (y posdoctorados) extranjeros del primero mundo vienen a trabajar con investigadores aquí. Creo que es muy importante recalcar este punto.

Por otro lado, he realizado colaboración (y tenido publicaciones) con estudiantes del primer mundo (varios de ellos realizando visitas a Uruguay) y estamos siguiendo en este camino. He sido reportero ("rapporteur") de 2 tesis de doctorado en Fancia en el marco de esta colaboración.

Creo que estamos avanzando muchísimo en los últimos años (ha sido realmente explosiva el crecimiento exponencial que hemos tenido en esta dirección y con la participación no sólo de estudiantes de grado y posgrado de Uruguay, sino también con investigadores de Matemática como Ezequiel Maderna en el último STIC-AMSUD RaPA2 que fue recientemente financiado) en este camino.

Estamos FIRMEMENTE convencidos que es el camino a seguir en cuanto "construcción institucional" en un mundo en cambio, con problemas serios de financiamiento local, en donde el rol de las Universidades está en proceso serio de cambio (debido a estar en un mundo integrado por las TICs) y en donde hay mucha participación estudiantil con mucho interes en estos temas teóricos, áridos y muy difíciles, en donde la colaboración con líderes internacionales es fundamental en este camino.

Tenemos mucho por delante, y un futuro esperanzador en momentos de crisis. Lo digo de corazón, y los hechos nos están dando la razón.

Información adicional

Uno de los motivos de mayor satisfacción tanto académica como personal es ver mucha gente jóven exitosa en diversos lugares del mundo, quienes de diversas maneras han valorado (!) y participado de actividades científicas que he impulsado y llevado adelante. Es el motivo principal por el cual, a pesar de la gran cantidad de situaciones adversas que he tenido que soportar, sigo por el momento trabajando en el país.
Mi actividad académica ha sido el motor que ha impulsado una amistad muy profunda con una gran cantidad de investigadores dispersos en diversos laboratorios científicos de primer nivel internacional. Por tal motivo, la publicación de trabajos conjuntos, la presentación y aprobación de proyectos de investigación y colaboración conjunta, la organización de eventos internacionales, las tutorías y co-tutorías de estudiantes y las periódicas visitas académicas son un motivo de gratos encuentros y muchas veladas que recordaremos y compartiremos toda la vida. Es claro que este vínculo tiene un impacto muy positivo en la calidad académica de nuestras publicaciones y de los estudiantes que han tomado nuestros cursos o han sido dirigidos en forma personal o en co-tutorías. Este valor agregado, es el principal motivo por el cual he podido salir adelante en mis actividades académicas en el país a pesar de todas las dificultades y contratiempos que he tenido.
Mis trabajos académicos editados, publicados y presentados incluyen coautores de los siguientes países: Argentina, Alemania, Bélgica, Canadá, Chile, China, Egipto, Eslovenia, España, Estados Unidos, Francia, Holanda, India, Inglaterra, Irán, México, Rusia, Suecia y Uruguay.
Siguiendo las indicaciones en http://algo.inria.fr/flajolet/numbers.html), mi número de Flajolet es 1, mi número de Erdös es 2 (http://www.oakland.edu/ grossman/erdoshp.html), mi número de Knuth es también 2 y mi número de Einstein es como máximo 7.
Desde 1991 a 1995 fui administrador de la primera mailing list de uruguayos que comunicó a más de 400 uruguayos en diversas partes del mundo. Muchas de las actividades de desarrollo cientifico - tecnológico - social, y de colaboración entre uruguayos radicados en el país y en el exterior surgieron de contactos hechos en dicha lista. La colaboración con los laboratorios HP es uno de los ejemplos más paradigmáticos.
Disfruto de los viajes y el aire libre. Son especialmente mencionables los momentos en La Floresta con mi familia, llena de niños y adolescentes, y con muchos amigos de diversas partes del mundo. Tenemos un cuaderno donde firma cada persona que se queda a dormir al menos una noche (una vez por cada estadía que haga) y en 17 años hemos coleccionado 675 firmas con gente de 22 países.
Una parte importante de mi investigación científica realizada con colaboración internacional fue

inspirada en este ambiente de trabajo.
En un momento tocaba guitarra, y espero retomar pronto. Como guitarrista y cantante soy un buen investigador en computación, pero me divierto.
Me gusta mucho jugar al bridge, y últimamente al Catan, aunque deseo de todo corazón poder jugarlo mejor!
Es un gusto asistir periódicamente a ver partidos de Defensor, tanto en el Uruguay como en el extranjero. En muchos aspectos para nada triviales, es un apostolado comparable al hacer investigación científica en Uruguay!

Indicadores de producción

PRODUCCIÓN BIBLIOGRÁFICA	**50**
Artículos publicados en revistas científicas	20
Completo	20
Trabajos en eventos	25
Libros y Capítulos	5
Libro publicado	4
Capítulos de libro publicado	1
PRODUCCIÓN TÉCNICA	**15**
Trabajos técnicos	4
Otros tipos	11
EVALUACIONES	**76**
Evaluación de proyectos	7
Evaluación de eventos	53
Evaluación de publicaciones	7
Evaluación de convocatorias concursables	5
Jurado de tesis	4
FORMACIÓN RRHH	**39**
Tutorías/Orientaciones/Supervisiones concluidas	37
Tesis de maestria	6
Tesis/Monografía de grado	25
Tesis de doctorado	2
Otras tutorías/orientaciones	4
Tutorías/Orientaciones/Supervisiones en marcha	2
Tesis de maestria	1
Tesis de doctorado	1