JUAN PEDRO HECHT

Profesor Titular de Criptografía

http://ar.linkedin.com/pub/juan-pedro-hecht/16/525/a6b/

Lic. en Análisis de Sistemas (ESIO-DIGID) y Doctor de la Universidad de Buenos Aires. Profesor Titular de Criptografía I/II de la Facultad de Ingeniería de la Escuela Superior Técnica (IUE), Profesor Titular de Biofísica (FO-UBA), Profesor Titular de Criptografía I / II y Coordinador Académico en el Posgrado y Maestría en Seguridad Informática de la Universidad de Buenos Aires, a cargo de las Facultades de Ciencias Exactas, Ciencias Económicas e Ingeniería.

Miembro representante de la Argentina en la Comisión Iberoamericana del Taller de Enseñanza de Seguridad de la Información.

Director de varios Proyectos de Investigación UBACyT (Universidad de Buenos Aires) sobre modelos matemáticos y de Criptografía.

Miembro de diversas sociedades científicas y profesionales.

Cotitular de la patente criptográfica argentina "*disposición y método para autenticar usuarios remotos*" AR N° P01-01-00047 (i.n.p.i.).y acreedor al Premio Segurinfo al mejor producto de Seguridad Informática (Marzo 2008).

Autor de numerosos trabajos en revistas especializadas de alto impacto, capítulos de libros y de un libro de texto sobre computación cuántica aplicada a la criptografía.

Es CTO de Firmas Digitales SRL empresa dedicada a los desarrollos criptográficos.

Director Titular de EUDEBA (Editorial de la Universidad de Buenos Aires) desde 2014 , referee y miembro del Editorial Board de la IEEE Transactions Latin America y miembro del comité de programa de numerosos Congresos Internacionales vinculados con la Criptografía, Inteligencia Computacional y Seguridad Informática.

Libros publicados

"Fundamentos de computación cuántica", Hecht, J. P., Editorial Académica Española,
LAP LAMBERT Academic Publishing GmbH & Co. KG (Printed in USA), 110 páginas, (2012)
ISBN 978-3-8484-7529-2

Capítulos de libros publicados

"A Zero-Knowledge authentication protocol using non commutative groups" Hecht, J. P. Actas del VI Congreso Iberoamericano de Seguridad Informática CIBSI'11, Ramió Aguirre J. el al (Eds), Universidad Politécnica de Madrid (España), 96-102 (2011) ISBN: 978-958-8506-18-0

"Criptografía no conmutativa usando un grupo general lineal de orden primo de Mersenne", P. Hecht, Actas del VII Congreso Iberoamericano de Seguridad Informática CIBSI'13, Ramió Aguirre J. el al (Eds), Universidad Politécnica de Madrid (España), 147-153 (2013) ISBN: 978-9962-676-43-0

"Primeros avances en el estudio de anillos en ataques cíclicos al criptosistema RSA", Hecht J.P., Ramió Aguirre J., Casado Gimeno A., Actas de la XIII Reunión Española sobre Criptología y Seguridad de la Información : celebrado del 5 al 8 de septiembre 2014, Alicante, pp. 19-24 (2014)
ISBN 978-84-9717-323-0 (URI: http://hdl.handle.net/10045/40389)

¿Por qué participar en el CIBSI / TIBETS?

Para presentar resultados de mis proyectos de investigación.

En su opinión, ¿cuál es la relevancia de su investigación en este Congreso?

Es relevante por los aportes absolutamente novedosos en el área de la criptografía post-cuántica. En los tres trabajos que presento, se trata de desarrollos de algoritmos y protocolos originales desarrollados para reemplazo de criptosistemas asimétricos vulnerables a los ataques de computadoras cuánticas.

¿Cuál piensa que será el devenir de la Seguridad de la Información?

Cada día más por la constante evolución de las informática en la Sociedad mundial

¿Cuál es el mayor riesgo que tiene una sociedad como la Iberoamericana en materia de ciberseguridad?

Ataques a la confidencialidad por parte de Agencias de Seguridad de las potencias del primer mundo, particularmente la NSA (USA) y sus socios estratégicos.

¿Cómo ve a Latinoamérica en materia de seguridad de la información frente al resto del mundo?

En pañales pero con vista a crecer en la próxima década.

ARTÍCULOS PRESENTADOS EN CIBSI-TIBETS 2015

A Post-Quantum Set of Compact Asymmetric Protocols using a General Linear Group. *Full Paper*

Zero-Knowledge Proof Authentication using Left Self Distributive Systems: a Post-Quantum Approach. *Full Paper*

A Diffie-Hellman Compact Model Over Non- Commutative Rings Using Quaternions. *Short Paper*

Miércoles, 11 Noviembre - Bloque Criptografía.

Universidad de Buenos Aires - ARGENTINA
Maestría en Seguridad Informática (Facultad de Ciencias Exactas y Naturales)
http://exactas.uba.ar/academico/display.php?estructura=2&desarrollo=0&id_caja=44&nivel_caja=2

Con la Organización de