SARA DÍAZ CARDELL

Investigadora pos-doctoral

http://www.researchgate.net/profile/Sara_Cardell

Su área de trabajo principal es la teoría de códigos. Ya en su tesis doctoral trataba sobre la construcción y estudio de códigos con máxima distancia de separación.

Después de terminar el doctorado, le fue concedida una beca pos-doctoral de dos años en la que estuvo trabajando entre la Universidad de Alicante y el CSIC (Madrid).

Durante su estancia de un año en en el CSIC, comenzó a trabajar en criptografía de clave privada con la investigadora Amparo Fúster. Uno de los frutos de esa colaboración es el trabajo que presenta este año en el CIBSI.

Actualmente está disfrutando de una beca pos-doctoral de FAPESP (con referencia 2015/07246-0) en la Universidad Estatal de Campinas (UNICAMP) en Brasil. Bajo la supervisión del profesor Marcelo Firer, sigue trabajando en teoría de códigos, pero sigue interesada en continuar trabajando y ampliando su conocimiento sobre criptografía y seguridad.

Entre sus publicaciones más importantes constan:

S. D. Cardell, D. Gómez-Pérez, J. Gutiérrez. *Generalized explicit inversive generators of small p-weight degree.* In *Finite Fields and their Applications*, 25: 316-325, 2014.

S.D. Cardell, J.-J., Climent, V. Requena. A *construction of MDS array codes. In WIT Transactions on Information and Communication Technologies* , 45: 47-58, 2013.

S. D. Cardell, J.-J., Climent. *A Performance of SPC product codes on the erasure channel.* Accepted in Advances of Mathematics in Communications (AMC), 2014.

S. D. Cardell, A. Fúster-Sabater. *Linear models for the self-shrinking generator based on CA.* Accepted in Journal of Cellular Automata, 2015.

Además de otros dos publicaciones que se encuentran bajo revisión.

¿Por qué participar en el CIBSI / TIBETS?

Hace poco que me incorporé en la UNICAMP y no conozco a las personas que trabajan en esta área en Sudamérica. Tengo intención de quedarme a trabajar aquí los próximos años y quiero aprovechar este congreso para hacer contactos y conocer a la gente que se dedica a la cripto y a la seguridad. Creo que este congreso es muy popular y prestigioso, y puede ser una gran oportunidad muy buena para darme a conocer en este ámbito.

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

En nuestro trabajo, Amparo y yo tratamos de romper generadores de secuencias cifrantes basados en decimación. Dada una secuencia generada por un LFSR (Linear Feedback Shift Register), esta secuencia tiene buenas propiedades criptográficas, pero dada su linealidad, no se pueden utilizar como secuencias cifrantes. Una solución por parte de los criptógrafos, fue utilizar estas secuencias como base para estructuras más complejas. Por ejemplo, los generadores basados en decimación, llamados shrinking, toman secuencias generadas por LFSR y las transforman en otras secuencias con alta complejidad lineal y alto periodo. A primera vista estas secuencias parecen aptas para usos criptográficos. Sin embargo, en nuestro trabajo, podemos observar cómo estas secuencias se pueden obtener también utilizando otras estructuras lineales. Dada esta linealidad, estos generadores podemos deducir que, a pesar del esfuerzo por romper la linealidad, estos generadores no son seguros.

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

Hoy en día, toda la información está en constante amenaza. El mundo de la informática está en constante evolución y cambio, cada día surgen amenazas nuevas y hay que intentar estar al día para poder evitar que nuestra información sea vulnerable ante estos ataques. Cada vez más, las personas se conciencian de que la información que manejan no es segura y cada vez, más expertos comienzan a trabajar en esta área. Creo que poco a poco la Seguridad de la información se va a convertir en un tema más y más popular atrayendo a personas de todos los países a participar en el desarrollo de nuevas herramientas que nos proporcionen la seguridad que necesitamos.

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

Creo que es posible que no estemos preparados para las amenazas que nos acechan. El mundo de la informática avanza muy deprisa y hay que intentar no quedarse retrasados. No hay que olvidar que nadie está libre de los ataques, y hay que concienciar cada vez más de la importancia de la seguridad de la información que manejamos. Hay que saber a qué nos enfrentamos y para eso todavía que un largo camino que recorrer.

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

Creo que Latinoamérica todavía no está al nivel de otros países, que quizás comenzaron a preocuparse por esta materia hace mucho más tiempo. Sin embargo creo que en los últimos años hemos podido observar un avance en cuanto a la concienciación sobre la importancia de la seguridad de la información. Además, creo que eventos como el CIBSI, que ponen en contacto personas y empresas que trabajan en esta materia, ayudan a que poco a poco Latinoamérica avance para ponerse al nivel que merece con respecto al resto del mundo.

ARTÍCULOS PRESENTADOS EN CIBSI-TIBETS 2015

Modelización lineal de generadores de secuencias basados en decimación. *Full Paper*

Miércoles, 11 Noviembre
Bloque Criptografía.

Universidade Estatual de Campinas (UNICAMP) - BRASIL
http://www.unicamp.br/unicamp/