



AMPARO FUSTER SABATER

Científico Titular del C.S.I.C.

Amparo Fuster Sabater (Madrid 1956) obtuvo su Licenciatura en Ciencias Físicas por la Universidad Complutense de Madrid en 1980, y su título de Doctor en Ciencias Físicas por la misma universidad en 1985.

Es investigador en el Departamento de Tratamiento de la Información y Criptografía (TIC) en el Instituto de Tecnologías Físicas y de la Información (ITEFI) del Consejo Superior de Investigaciones Científicas (CSIC) en Madrid.

Ha participado en más de 30 proyectos de investigación. Es autora de varios libros y patentes, más de 150 artículos en revistas especializadas, más de 100 contribuciones a Congresos, ha dirigido varias tesis doctorales y es revisora y revisora de diferentes revistas indexadas en el SCI y de numerosos congresos internacionales.

Es asimismo co-fundadora de la Reunión Española de Criptología y Seguridad de la Información (RECSI), reunión bianual que inició su singladura en 1991 y que ya ha celebrado su XIII edición.

Sus actuales líneas de investigación incluyen la Criptografía y Seguridad de la información, con particular énfasis en Criptografía de clave secreta, Criptoanálisis, Seguridad en redes inalámbricas y Autómatas celulares.

Es consultora del Centro Criptológico Nacional dependiente del Centro Nacional de Inteligencia (CNI) en materia de Criptografía de clave secreta y cifrado en flujo.

¿Por qué participar en el CIBSI / TIBETS?

Es un congreso iberoamericano relacionado con mi actividad profesional. Siempre que me ha sido posible he participado en la correspondiente edición y pienso seguir haciéndolo en el futuro.

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

Presentamos una ponencia "Modelización lineal de generadores de secuencias basados en decimación" donde desarrollamos una técnica de linealización que permite criptoanalizar toda una familia de generadores de secuencias criptográficas. Supone, esencialmente, una contribución al criptoanálisis de cifradores en flujo.

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

Una ciencia fundamental en nuestros días que irá ampliando su campo de acción a todos los sectores de la vida cotidiana.

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

El mismo que en cualquier otro ámbito geográfico: grandes cantidades de información sensible que hay que proteger y numerosos grupos y sociedades delictivas que, sin ningún escrúpulo, intentan obtenerla y hacer uso de ella.

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

En cuestión de seguridad creo que tiene un nivel muy adecuado, podríamos decir que está en la media alta. Eso no quita para que todavía se pueda llevar a cabo una gran labor. A nivel criptográfico creo que todavía hay mucho por hacer y que un congreso tipo CIBSI/TIBET puede contribuir a esta mejora.

ARTÍCULOS PRESENTADOS EN CIBSI-TIBETS 2015

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

Miércoles, 11 Noviembre
Bloque Criptografía.