Matemática contemporánea por matemáticas contemporáneas, Maribel González Vasco

Desde la RSME queremos visibilizar el papel de las mujeres en las matemáticas. Para ello, y aprovechando la celebración del Día de la Mujer Trabajadora, vamos a difundir semanalmente el perfil de una mujer matemática en el Boletín de la RSME. Estos perfiles han sido elegidos para una exposición, coordinada por Rosa María Pardo San Gil del departamento de Matemática Aplicada de la Universidad Complutense de Madrid, que se exhibirá en las facultades de las bibliotecas de todas las facultades españolas que cuenten con estudios de matemáticas, y queremos colaborar con su difusión.

Maribel González Vasco Maribel González Vasco es profesora titular de Matemática Aplicada de la Universidad Rey Juan Carlos. Licenciada en Matemáticas y doctora por la Universidad de Oviedo, ha desarrollado su carrera investigadora colaborando con distintos centros públicos y privados (Philips Crypto; Institut fu r Algorithmen und Kognitive Systeme de la Universität Karlsruhe, Alemania; CCIS Florida, e Imdea Software, Madrid). Ha publicado más de cuarenta artículos en revistas indexadas y congresos de prestigio, y liderado proyectos de investigación básica y contratos de transferencia a empresas. Es miembro de la IACR (International Association for Cryptologic Research) y vocal de la Junta de Gobierno de la Real Sociedad Matemática Española.Su área de trabajo es la criptografía matemática. En criptoanálisis (análisis críptológico) destacan sus resultados identificando vulnerabilidades en esquemas de cifrado construidos a partir de teoría de grupos, así como señalando problemas en protocolos para intercambio de clave en entornos multiusuario. Entre sus trabajos constructivos destacan sus propuestas para intercambio de clave en grupo sin firma digital, su trabajo en modelos para reutilizar claves de manera segura y sus trabajos en privacidad en operaciones conjuntistas.Artículos:

- M. I. González Vasco, F. Hess y R. Steinwandt. “Combined schemes for signature and encryption: The public-key and the identity-based setting”. Information and Computation 247 (2016). Págs. 1-10.
- D. Fiore, M. I. González Vasco y C. Soriente. “Partitioned Group Password-Based Authenticated Key Exchange”. The Computer Journal 60-12 (2017). Págs. 1912-1922.
- P. d’Arco, M. I. González Vasco, A. L. Pérez del Pozo, C. Soriente y R. Steinwandt. “Private set intersection: New generic constructions and feasibility results”. Advances in Mathematics of Communications 11-3 (2017). Págs. 481-502.