CONGRESO DE JÓVENES INVESTIGADORES
Real Sociedad Matemática Española
Universidad de Murcia, del 7 al 11 de Septiembre de 2015

Non-interactive identity-based 3-party key distribution

Adriana Suárez Corona[1], **Rainer Steinwandt**[2]

A Non-interactive Key Exchange scheme allows parties to compute a shared common key without any interaction. Pairing-friendly curves and elliptic curves with a trapdoor for the discrete logarithm problem are versatile tools in the design of cryptographic protocols. We show that curves having both properties simultaneously would yield a non-interactive solution for identity-based 3-party key distribution in the random oracle model, based on the hardness of the Bilinear Diffie-Hellman Problem.

[1]Departmento de Matemática Aplicada
Universidad de León
Escuela de Ingenierías Industrial e Informática Campus de Vegazana s/n, 24071 LEÓN
asuac@unileon.es

[2]Department of Mathematical Sciences
Florida Atlantic University
777 Glades Road, Boca Raton, FL 33431
rsteinwa@fau.edu