Published in T. Muntean, R. Rolland, and D. Poulakis, Eds, *Algebraic Informatics (CAI 2013)*, vol. 8080 of *Lecture Notes in Computer Science*, p. 6, Springer, 2013.

On Elliptic Curve Paillier Schemes

(Invited Talk)

Marc Joye

Technicolor, France
marc.joye@technicolor.com

Abstract. In 1999, Paillier proposed an elegant cryptosystem from the integers modulo N^2 where N is an RSA modulus. Paillier public-key encryption scheme enjoys a number of interesting properties, including a homomorphic property: the encryption of two messages allows anyone to derive the encryption of their sum. This reveals useful in cryptographic applications such as electronic voting. In this talk we review several generalizations of the original Paillier scheme to the elliptic curve setting. Using similar ideas, we then present a new elliptic curve scheme which is semantically secure in the standard model. Interestingly, the new encryption scheme does not require to encode messages as points on an elliptic curve and features a partial homomorphic property.