Published In W. Meier and D. Mukhopadhyay, Eds., *Progress in Cryptology – INDOCRYPT 2014*, vol. 8885 of *Lecture Notes in Computer Science*, p. XXI, Springer, 2014.

Recent Advances in ID-based Encryption
(Invited Talk)

Marc Joye

Technicolor, USA
marc.joye@technicolor.com

Abstract. Most ID-based cryptosystems make use of bilinear maps. A notable exception is a 2001 publication by Clifford Cocks describing an ID-based cryptosystem that works in standard RSA groups. Its semantic security relies on the quadratic residuosity assumption. Cocks's publication gave rise to several follow-up works aiming at improving the original scheme in multiple directions. This talk reviews Cocks' scheme and presents its known variants and extensions. It also discusses applications thereof. Finally it reports some recent developments the author made in the area.