Chen, Jie; **Wee, Hoeteck**

Fully, (almost) tightly secure IBE and dual system groups. (English) Zbl 1311.94072

Canetti, Ran (ed.) et al., Advances in cryptology – CRYPTO 2013. 33rd annual cryptology conference, Santa Barbara, CA, USA, August 18–22, 2013. Proceedings, Part II. Berlin: Springer (ISBN 978-3-642-40083-4/pbk). Lecture Notes in Computer Science 8043, 435-460 (2013).

Summary: We present the first fully secure identity-based encryption scheme (IBE) from the standard assumptions where the security loss depends only on the security parameter and is independent of the number of secret key queries. This partially answers an open problem posed by *B. Waters* [Eurocrypt 2005, Lect. Notes Comput. Sci. 3494, 114–127 (2005; Zbl 1137.94360)]. Our construction combines the Waters' dual system encryption methodology [*B. Waters*, Crypto 2009, Lect. Notes Comput. Sci. 5677, 619–636 (2009; Zbl 1252.94101)] with the Naor-Reingold pseudo-random function [*M. Naor* and *O. Reingold*, J. ACM 51, No. 2, 231–262 (2004; Zbl 1248.94086)] in a novel way. The security of our scheme relies on the DLIN assumption in prime-order groups. Along the way, we introduce a novel notion of dual system groups and a new randomization and parameter-hiding technique for prime-order bilinear groups.

For the entire collection see [Zbl 1270.94006].

Reviewer: Reviewer (Berlin)

MSC:

94A60 Cryptography

Full Text: DOI