Boneh, Dan; **Katz, Jonathan**

Improved efficiency for CCA-secure cryptosystems built using identity-based encryption.
(English) Zbl 1079.94535

Menezes, Alfred (ed.), Topics in cryptology – CT-RSA 2005. The cryptographers' track at the RSA conference 2005, San Francisco, CA, USA, February 14–18, 2005. Proceedings. Berlin: Springer (ISBN 3-540-24399-2/pbk). Lecture Notes in Computer Science 3376, 87-103 (2005).

Summary: Recently, R. Canetti, S. Halevi, and J. Katz showed a general method for constructing CCA-secure encryption schemes from identity-based encryption schemes in the standard model. We improve the efficiency of their construction, and show two specific instantiations of our resulting scheme which offer the most efficient encryption (and, in one case, key generation) of any CCA-secure encryption scheme to date.

For the entire collection see [Zbl 1069.94501].

MSC:

94A60 Cryptography

Keywords:

Chosen-ciphertext security; Identity-based encryption; Public-key encryption

Full Text: DOI