Seo, Jae Hong; **Kobayashi, Tetsutaro**; **Ohkubo, Miyako**; **Suzuki, Koutarou**

Anonymous hierarchical identity-based encryption with constant size ciphertexts. (English)

Zbl 1227.94064

Jarecki, Stanisław (ed.) et al., Public key cryptography – PKC 2009. 12th international conference on practice and theory in public key cryptography, Irvine, CA, USA, March 18–20, 2009. Proceedings. Berlin: Springer (ISBN 978-3-642-00467-4/pbk). Lecture Notes in Computer Science 5443, 215-234 (2009).

Summary: We propose an anonymous Hierarchical Identity-Based Encryption (anonymous HIBE) scheme that has constant size ciphertexts. This means the size of the ciphertext does not depend on the depth of the hierarchy. Moreover, our scheme achieves the lowest computational cost because during the decryption phase the computational cost of decryption is constant. The security can be proven under reasonable assumptions without using random oracles because it is based on the composite order bilinear group. Our scheme achieves selective-ID security notion.

For the entire collection see [Zbl 1157.94004].

MSC:

94A60 Cryptography

Full Text: DOI