Boneh, Dan; **Canetti, Ran**; **Halevi, Shai**; **Katz, Jonathan**
Chosen-ciphertext security from identity-based encryption. (English) Zbl 1138.94010
SIAM J. Comput. 36, No. 5, 1301-1328 (2006).

The present paper illustrates a CCA-Secure public-key encryption scheme which can be used in a real condition of chosen cipher text attacks. The article is very well structured and all the used techniques have a good bibliography and proofs. There are other techniques in information security which achieve the same aim, but the current exposed one has its own originality.

Reviewer: Nicolae Constantinescu (Craiova)

MSC:

94A60 Cryptography
68P25 Data encryption (aspects in computer science)

Keywords:

public key encryption; cryptographic attack

Full Text: DOI