Osin, Denis; **Shpilrain, Vladimir**

Public key encryption and encryption emulation attacks. (English) Zbl 1142.94356

Hirsch, Edward A. (ed.) et al., Computer science – theory and applications. Third international computer science symposium in Russia, CSR 2008 Moscow, Russia, June 7–12, 2008. Proceedings. Berlin: Springer (ISBN 978-3-540-79708-1/pbk). Lecture Notes in Computer Science 5010, 252-260 (2008).

Summary: The main purpose of this paper is to suggest that public key encryption can be secure against the "encryption emulation" attack (on the sender's encryption) by computationally unbounded adversary, with one reservation: a legitimate receiver decrypts correctly with probability that can be made arbitrarily close to 1, but not equal to 1.

For the entire collection see [Zbl 1136.68005].

MSC:

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

Full Text: DOI