Fiat, Amos; **Shamir, Adi**

How to prove yourself: Practical solutions to identification and signature problems. (English)

Zbl 0636.94012

Advances in cryptology - CRYPTO '86, Proc. Conf., Santa Barbara/Calif. 1986, Lect. Notes Comput. Sci. 263, 186-194 (1987).

Summary: In this paper we describe simple identification and signature schemes which enable any user to prove his identity and the authenticity of his messages to any other user without shared or public keys. The schemes are provably secure against any known or chosen message attack if factoring is difficult, and typical implementations require only 1% to 4% of the number of modular multiplications required by the RSA scheme. Due to their simplicity, security and speed, these schemes are ideally suited for microprocessor-based devices such as smart cards, personal computers, and remote control systems.

For the entire collection see Zbl 0624.00026.

MSC:

94A60 Cryptography
94A62 Authentication, digital signatures and secret sharing

Keywords:

identification and signature schemes; authentication; security

Full Text: DOI