Yoon, Eun-Jun; Yoo, Kee-Young
Robust user password change scheme based on the elliptic curve cryptosystem. (English)
Zbl 1154.94441

Summary: In this paper, an efficient user password change scheme based on the elliptic curve discrete logarithm problem (ECDLP) is presented. In contrast to the existing password change schemes using a server’s public key, the proposed scheme can securely update user passwords without a complicated process and server’s public key, and also provides explicit key authentication in the case of a session key agreement.

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