Cao, Yang; Li, Na; Pan, Jiqiang; Da, Liexiong
Dynamic authentication key agreement protocol based on chaos mapping.  (Chinese. English summary) Zbl 07448810

Summary: In order to solve the security problems in key negotiation, combining with the good cipher features of chaos mapping, this paper proposes a mutual key negotiation protocol for dynamic authentication. In the protocol, the user's identity for each key negotiation is dynamic, which can resist impersonation attack and replay attack while realizing user anonymity. The addition/decryption algorithm and clock synchronization are not used in the key negotiation, which reduces the complexity of protocol execution and improves the operation efficiency. The security is based on the unipolarity of hash function, extended Chebyshev polynomial discrete logarithm problems, and Diffie-Hellman problem. It can be seen from the security analysis that this protocol can resist common attacks and has high security. It can be seen from the performance analysis that the protocol has lower transmission complexity and computational complexity. It is suitable for practical application environment.

MSC:
68M12 Network protocols
68P25 Data encryption (aspects in computer science)

Keywords:
chaotic map; key agreement; authentication; dynamic identity; discrete logarithm problems; Diffie-Hellman problem