World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:18, No:08, 2024

A Novel Unconditionally Secure and Lightweight Bipartite Key Agreement Protocol

Authors : Jun Liu

Abstract : This paper introduces a new bipartite key agreement (2PKA) protocol which provides unconditionally security and lightweight. The unconditional security is stemmed from the known impossibility of distinguishing a particular solution from all possible solutions of an underdetermined system of equations. The indistinguishability prevents an adversary from inferring to the common secret-key even with the access to an unlimited amount of computing capability. This new 2PKA protocol is also lightweight because that the calculation of a common secret-key only makes use of simple modular arithmetic. This information-theoretic 2PKA scheme provides the desired features of Key Confirmation (KC), Session Key (SK) security, Know-Key (KK) security, protection of individual privacy, and uniformly distributed value of a common key under prime modulus.

Keywords : bipartite key agreement, information-theoretic cryptography, perfect security, lightweight
Conference Title : ICAC 2024 : International Conference on Applied Cryptography
Conference Location : Venice, Italy
Conference Dates : August 15-16, 2024

Open Science Index, Computer and Information Engineering Vol:18, No:08, 2024 publications.waset.org/abstracts/178770.pdf