World Academy of Science, Engineering and Technology
International Journal of Mathematical and Computational Sciences
Vol:13, No:01, 2019

Key Transfer Protocol Based on Non-invertible Numbers

Authors : Luis A. Lizama-Perez, Manuel J. Linares, Mauricio Lopez

Abstract : We introduce a method to perform remote user authentication on what we call non-invertible cryptography. It exploits the fact that the multiplication of an invertible integer and a non-invertible integer in a ring Zn produces a non-invertible integer making infeasible to compute factorization. The protocol requires the smallest key size when is compared with the main public key algorithms as Diffie-Hellman, Rivest-Shamir-Adleman or Elliptic Curve Cryptography. Since we found that the unique opportunity for the eavesdropper is to mount an exhaustive search on the keys, the protocol seems to be post-quantum.

Keywords : invertible, non-invertible, ring, key transfer
Conference Title : ICCCIS 2019 : International Conference on Coding, Cryptology and Information Security
Conference Location : Paris, France
Conference Dates : January 24-25, 2019