Overcoming 4-to-1 Decryption Failure of the Rabin Cryptosystem

Authors : Muhammad Rezal Kamel Ariffin, Muhammad Asyraf Asbullah

Abstract : The square root modulo problem is a known primitive in designing an asymmetric cryptosystem. It was first attempted by Rabin. Decryption failure of the Rabin cryptosystem caused by the 4-to-1 decryption output is overcome efficiently in this work. The proposed scheme to overcome the decryption failure issue (known as the AAβ-cryptosystem) is constructed using a simple mathematical structure, it has low computational requirements and would enable communication devices with low computing power to deploy secure communication procedures efficiently.

Keywords : Rabin cryptosystem, 4-to-1 decryption failure, square root modulo problem, integer factorization problem

Conference Title : ICCCISE 2015 : International Conference on Computer, Communication and Information Sciences, and Engineering

Conference Location : Jeddah, Saudi Arabia

Conference Dates : January 26-27, 2015