Provably secure Rabin-p cryptosystem in hybrid setting

ABSTRACT

In this work, we design an efficient and provably secure hybrid cryptosystem depicted by a combination of the Rabin-p cryptosystem with an appropriate symmetric encryption scheme. We set up a hybrid structure which is proven secure in the sense of indistinguishable against the chosen-ciphertext attack. We presume that the integer factorization problem is hard and the hash function that modeled as a random function.

Keyword: Hybrid cryptosystem; Rabin-p cryptosystem; Security