Provably secure randomized AAβ cryptosystem

ABSTRACT

The security of a modern public key cryptosystem is usually viewed from their security goal and attack models, with the intention to come out with a provably secure cryptosystem. In this paper, we propose a randomized encryption setting algorithm based on the AAɓ cryptosystem. We also present provable security elements for the randomized AAɓ cryptosystem with emphasis given to the standard security against strongest attack model, namely the chosen-ciphertext attack. This randomized AAɓ cryptosystem is projected in the random oracle model.

Keyword: AAɓ cryptosystem; Provable security; Chosen ciphertext attack; Random oracle model