

A Trapdoor Permutation Equivalent to Factoring and Its Applications

Katja Schmidt-Samoa

Technische Universität Darmstadt, Fachbereich Informatik,
Hochschulstr. 10, D-64289 Darmstadt, Germany
`samoa@informatik.tu-darmstadt.de`

Abstract. Public key cryptography has been invented to overcome some key management problems in open networks. Although nearly all aspects of public key cryptography rely on the existence of trapdoor one-way functions, only a very few candidates of this primitive have been observed yet. In this paper, we introduce a new trapdoor one-way permutation based on the hardness of factoring integers of p^2q -type. We also propose a variant of this function with a different domain that provides some advantages for practical applications. To confirm this statement, we develop a simple hybrid encryption scheme based on our proposed trapdoor permutation that is CCA-secure in the random oracle model.

Keywords: trapdoor one-way permutations, EPOC, hybrid encryption, Tag-KEM/DEM framework