Cryptanalysis of a public key cryptosystem based on boolean permutations

Esam Elsheh*
Amr Youssef†
Concordia Institute for Information Systems Engineering
Concordia University Montr´eal, QC, H3G 2W1
Canada

Abstract

Several attempts were made to construct public key cryptosystems based on Boolean permutations. Wu and Varadharajan proposed three such constructions (PKC1, PKC2 and PKC3) whose security is based on the difficulty of inverting a special class of trapdoor Boolean permutations that can be constructed efficiently. In this paper, we analyze the security of the PCK2 family proposed by Wu and Varadharajan. In particular, we show that the suggested construction for the PCK2 family is insecure and we present an efficient cryptanalytic attack that allows the cryptanalyst to invert the class of Boolean permutations used in PCK2 without the knowledge of the secret key parameters.

Keywords: *Public key cryptography; Boolean permutation; cryptanalysis.*