CORR 2000-60

Cryptanalysis of a Public Key Cryptosystem Using Matrices Over a Ring

A.M. Youssef & G. Gong*

Abstract At ACISP 2000, Yoo *et al* proposed a fast public key cryptosystem using matrices over a ring. The authors claim that the security of their system is based on the RSA problem. In this paper we present a heuristic attack that enables us to recover the private key from the public key. In particular, we show that breaking the system can be reduced to finding a short vector in a lattice which can be achieved using L^3-lattice reduction algorithm.

Keywords public key cryptography, cryptanalysis, L^3-algorithm.