CORR 2000-29

Cryptanalysis of Imai and Matsumoto scheme B asymmetric cryptosystem

A.M. Youssef

Abstract Imai and Matsumoto introduced alternative algebraic methods for constructing public key cryptosystems. An obvious advantage of these public key cryptosystems is that the private side computations can be made very efficient with a simple hardware. Almost all of these proposals and variants of them were broken. However, scheme "B" in [3] is still unbroken. In this paper we show some statistical weaknesses of this scheme. We also represent a cryptanalytic attack that enables the cryptanalyst to decrypt, with high probability, a given ciphertext by performing a very limited number of encryption operations using the public encryption function.

Keywords Public-key cryptosystems, cryptanalysis, Imai and Matsumoto asymmetric cryptosystems