Algebraic analysis of a rabin-like cryptosystem and its countermeasures

ABSTRACT

Objective: In this paper, we present two algebraic analyses upon a new Rabin-like public key cryptosystem namely the Rabin-p cryptosystem. Methods/Analysis: We show that by using the continued fraction's method and the Coppersmith's theorems, there exists inappropriate parameter's size that can affect the security of Rabin-p cryptosystem. Findings: The first analysis proved that the prime factors of its public key can be found amongst the list of the continued fraction expansion of the ciphertext c and the modulus N=p2q in polynomial time. For the second analysis, by using the Coppersmith's theorems we showed that the message m can be retrieved in polynomial time provided some condition on the message length. We also propose a countermeasure to avoid both analyses. Novelty/Improvement: The purpose of this work is to offer suggestions for a countermeasure for the aforementioned analysis upon implementing the Rabin-p cryptosystem. Hence, all the parameters should be chosen carefully.

Keyword: Rabin-pcryptosystem; Continued fraction; Coppersmith's theorems; Algebraic analysis