Abstract

In 2002, de Weger showed that choosing an RSA modulus with a small difference of primes improves the attack given by Boneh-Durfee. For this attack, de Weger used the complicated geometrical progressive matrices, introduced by Boneh-Durfee. In this paper, we analyzed by using another technique called unravelled linearization.
Cryptanalysis of RSA with Small Prime Difference using Unravelled Linearization

- Victor Shoup. NTL: A library for doing number theory. Website: http://www.shoup.net/ntl/.

Index Terms
Computer Science Security

Keywords
Lattice reduction RSA Cryptanalysis Unravelled linearization