Cryptology ePrint Archive: Report 2011/477

Cryptanalysis of NTRU with two public keys

Abderrahmane Nitaj

Abstract: NTRU is a fast public key cryptosystem presented in 1996 by Hoffstein, Pipher and Silverman. It operates in the ring of truncated polynomials. In NTRU, a public key is a polynomial defined by the combination of two private polynomials. In this paper, we consider NTRU with two different public keys defined by different private keys. We present a lattice-based attack to recover the private keys assuming that the public keys share polynomials with a suitable number of common coefficients.

Category / Keywords: public-key cryptography / NTRU cryptosystem; Lattice attacks; Cryptanalysis;

Date: received 2 Sep 2011

Contact author: abderrahmane nitaj at unicaen fr

Available formats: PDF | BibTeX Citation

Version: 20110906:040604 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]