Cryptology ePrint Archive: Report 2011/590

An Efficient Broadcast Attack against NTRU

Jianwei Li and Yanbin Pan and Mingjie Liu and Guizhen Zhu

Abstract: The NTRU cryptosystem is the most practical scheme known to date. In this paper, we first discuss the ergodic-linearization algorithm against GGH, then naturally deduce a new and uniform broadcast attack against several variants of NTRU: for every recipient’s ciphertext, isolate out the blinding value vector, then do derandomization directly and entirety by using inner product, afterwards by using some properties of circular matrix together with linearization we obtain three linear congruence equations of the form aTY = s mod q0 with N + [N2] variables. Hence only if the number of the independent recipients’ ciphertexts/public-keys pairs reaches N + [N2] &#8722; 2 can we work out these variables and recover the plaintext in O(N3) arithmetic operations successfully. The experiment evidence indicates that our algorithm can efficiently broadcast attack against NTRU with the highest security parameters. To the best of our knowledge, this is the most efficient broadcast attack against NTRU. This is an algebraic broadcast attack, which is based on the special structure of the blinding value space Lr.

Category / Keywords: Broadcast attack, NTRU, GGH, derandomization, linerization, circular matrix

Date: received 30 Oct 2011, last revised 24 Nov 2011

Contact author: lijianwei10 at mails tsinghua edu cn

Available formats: PDF | BibTeX Citation

Version: 20111124:111024 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]