

New NTRUEncrypt parameters and padding scheme

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2003-06/1455.html>

From: William Whyte (wwhyte_at_ntru.com)

Date: 06/27/03

Date: 27 Jun 2003 13:17:03 -0700

NTRU Cryptosystems has posted several new documents, which are available through <http://www.ntru.com/cryptolab/params.htm>.

As background: recent results on NTRUEncrypt have shown that decryption failures on validly encrypted messages leak information that eventually allows an attacker to recover the private key. The results do not affect the known difficulty of the underlying class of lattice problems; however, they show that care must be taken in choosing parameters to ensure that decryption failures occur with negligible or zero probability, even in the presence of an adversary who is actively trying to cause such failures.

NTRU Cryptosystems is proposing slightly altered parameter sets which decrease the probability of average-case decryption failures, and a padding scheme which ensures that an attacker cannot increase the probability of decryption failures above this average-case probability.

The new documents analyze the strength of the new parameter sets against all known attacks on NTRU (lattice-based, meet-in-the-middle, and decryption failure based) and show that for $N=251$ we comfortably achieve 2^{80} security against all of these attacks. We also provide the first ever full proof of security to be presented for NTRUEncrypt.

If anyone has any questions, I'll be happy to answer them.

Cheers,

William

=====
William Whyte
Director, Cryptographic R&D
NTRU Cryptosystems
5 Burlington Woods

sci.crypt: New NTRUEncrypt parameters and padding scheme

Burlington, MA 01803

tel: +1.781.418.2500

fax: +1.781.418.2532