CORR 2003-01

Imperfect Decryption and an Attack on the NTRU Encryption Scheme

John A. Proos

Abstract A property of the NTRU public-key cryptosystem is that it does not provide perfect decryption. That is, given an instance of the cryptosystem, there exist ciphertexts which can be validly created using the public key but which can't be decrypted using the private key. The valid ciphertexts which an NTRU secret key will not correctly decipher determine, up to a cyclic shift, the secret key. In this paper we present attacks based on this property against the NTRU primitive and many of the suggested NTRU padding schemes [15, 10, 11]. These attacks use an oracle for determining if valid ciphertexts can be correctly deciphered, and recover the user's secret key. The attacks are quite practical. For example, the attack against the NTRU-REACT padding scheme proposed in [15] with the $N = 503$ parameter set [21] requires on average fewer than 30,000 oracle calls and can be performed on a PC in a few minutes. As the traditional definition of a public-key encryption scheme requires perfect decryption, we also define a new type of encryption scheme which encompasses both NTRU and an attack model for the attacks presented against it.