NTRU: A Ring-Based Public Key Cryptosystem

Jeffrey Hoffstein, Jill Pipher, Joseph H. Silverman

ABSTRACT. We describe NTRU, a new public key cryptosystem. NTRU features reasonably short, easily created keys, high speed, and low memory requirements. NTRU encryption and decryption use a mixing system suggested by polynomial algebra combined with a clustering principle based on elementary probability theory. The security of the NTRU cryptosystem comes from the interaction of the polynomial mixing system with the independence of reduction modulo two relatively prime integers p and q.

CONTENTS

§0. Introduction

There has been considerable interest in the creation of efficient and computationally inexpensive public key cryptosystems since Diffie and Hellman [3] explained how such systems could be created using one-way functions. Currently, the most widely used public key system is RSA, which was created by Rivest, Shamir and Adelman in 1978 [9] and is based on the difficulty of factoring large numbers. Other systems include the McEliece system [8] which relies on error correcting codes, and a recent system of Goldreich, Goldwasser, and Halevi [4] which is based on the difficulty of lattice reduction problems.

In this paper we describe a new public key cryptosystem, which we call the NTRU system. The encryption procedure uses a mixing system based on polynomial algebra and reduction modulo two numbers p and q, while the decryption procedure uses an unmixing system whose validity depends on elementary probability theory. The security of the NTRU public key cryptosystem comes from the interaction of the polynomial mixing system with the independence of reduction modulo p and q. Security also relies on the (experimentally observed) fact that for most lattices, it is very difficult to find extremely short (as opposed to moderately short) vectors.

We mention that the presentation in this paper differs from an earlier, widely circulated but unpublished, preprint [6] in that the analysis of lattice-based attacks has been expanded and clarified, based largely on the numerous comments received from Don Coppersmith, Johan Håstad, and Adi Shamir in person, via email, and in the recent article [2]. We would like to take this opportunity to thank them for their interest and their help.

NTRU fits into the general framework of a probabilistic cryptosystem as described in [1] and [5]. This means that encryption includes a random element, so each message has many possible encryptions. Encryption and decryption with NTRU are extremely fast, and key creation is fast and easy. See Section 5 for specifics, but we note here that NTRU takes $O(N^2)$ operations to encrypt or decrypt a message block of length N, making it considerably faster than the $O(N^3)$ operations required by RSA. Further, NTRU key lengths are $O(N)$, which compares well with the $O(N^2)$ key lengths required by other "fast" public keys systems such as [8, 4].

§1. Description of the NTRU algorithm

§1.1. Notation. An NTRU cryptosystem depends on three integer parameters (N, p, q) and four sets $\mathcal{L}_f$, $\mathcal{L}_g$, $\mathcal{L}_\phi$, $\mathcal{L}_m$ of polynomials of degree $N-1$ with integer coefficients. Note that p and q need not be prime, but we will assume that $\gcd(p,q) = 1$, and q will always be considerably larger than p. We work in the ring $R = \mathbb{Z}[X]/(X^N - 1)$. An element $F \in R$ will be written as a polynomial or a vector,

$$F = \sum_{i=0}^{N-1} F_i x^i = [F_0, F_1, \ldots, F_{N-1}].$$

We write $\circledast$ to denote multiplication in R. This *star multiplication* is given