**Hoffstein, Jeffrey**; **Pipher, Jill**; **Silverman, Joseph H.**

**NTRU: A ring-based public key cryptosystem.** (English) Zbl 1067.94538

Buhler, J. P. (ed.), Algorithmic number theory. 3rd international symposium, ANTS-III, Portland, OR, USA, June 21–25, 1998. Proceedings. Berlin: Springer (ISBN 3-540-64657-4). Lect. Notes Comput. Sci. 1423, 267-288 (1998).

Summary: 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 $q$.

For the entire collection see [Zbl 0891.00022].

**MSC:**

94A60 Cryptography



**Software:**

NTRU

**Full Text:** Link