Report on Present State of NTRU Cryptosystem Evaluation (screening evaluation)

January 28, 2002

Jun Kogure, Member

Public-Key Cryptography Subcommittee

NTRU cryptosystem
(submitter's claims)

- Category: Confidentiality
- Security basis: CML (Convolution Modular Lattice) SVP (Shortest Vector Problem)
- Provable security: (1) IND-CPA conversion of primitives using random padding; (2) IND-CCA2 conversion using Fujisaki-Okamoto processing (assumes random oracle model)
- Characteristics: Fast encryption/decryption
- SW implementation information:
  Pentium III 800MHz, Palm Vx 20MHz,
  RIM 20MHz , ARM7 37MHz

Screening evaluation status
(evaluation of specifications)

The following areas need to be clarified:

- Parameter design criteria
- Required specifications for basic functions and auxiliary functions
- Evaluation of secret key generation success probability
- Evaluation of increase in ciphertext

Screening evaluation status
(security evaluation)

The following areas need to be checked in greater detail:

- Suitability of parameter design policy
- Conversion of random-padded primitives to IND-CPA
- Possibility of shortcut solutions