NTRU Cryptosystems Technical Report

Report # 005, Version 1
Title: Hard Problems and Backdoors for NTRU and Other PKCS's
Author: Joseph H. Silverman
Release Date: October 5, 1997

Abstract. A hard problem and the associated back door for the NTRU Public Key Cryptosystem is described and compared/contrasted with the hard problems and back doors associated to other common public key cryptosystems.

NTRU Public Key Cryptosystem

Hard Problem. The hard problem underlying the NTRU PKCS is to find a vector in a lattice (of large dimension) which is close to a given vector.

Backdoor. Knowledge of a small vector in the public lattice (i.e, a vector close to $\mathbf{0}$) allows the construction of a larger private lattice in which it is easy (by a two-step process) to find lattice vectors which are closest to certain given vectors.

RSA Public Key Cryptosystem

Hard Problem. The hard problem underlying the RSA PKCS is to find k^{th} roots modulo a composite integer N.

Backdoor. Knowledge of a factorization of N into primes allows one to find k^{th} roots modulo N by computing a reciprocal of k modulo $\phi(N)$.

El Gamel-Type Public Key Cryptosystems

Hard Problem. The hard problem underlying El Gamel-Type PKCS's is the discrete logarithm problem. Given two elements a and b in a (large) finite group, the discrete logarithm problem asks for the exponent k for which $a^k = b$ in the group.

Backdoor. The backdoor is knowledge of the exponent k.

GGH Lattice Public Key Cryptosystem

Hard Problem. The hard problem underlying the GGH PKCS (developed by Goldreich, Goldwasser, and Halevi) is to find a vector in a lattice (of large dimension) which is closest to a given non-lattice vector.

Backdoor. The backdoor is knowledge of a short (almost orthogonalized) basis for the lattice.

McEliece Public Key Cryptosystem

Hard Problem. The hard problem underlying the McEliece PKCS is given a k-dimensional subspace C of the vector space $\mathbf{F}_2^n$ and given a vector $\mathbf{x}$ not in C, find the vector in C closest of $\mathbf{x}$.

Backdoor. The backdoor is the use of a type of subspace C called a Goppa code in which the "nearest neighbor" problem can be efficiently solved. To prevent attack, the Goppa code matrix is disguised by multiplying by a random invertible matrix and a random permutation matrix (on left and right respectively) to create a public key matrix C' in which the nearest neighbor problem appears to be difficult to solve.

Expanded Description of the NTRU PKCS

The following remarks expand on the description of the NTRU PKCS.

Public Key. The public key is a lattice of dimension $2N$ which may be described as the lattice generated by the columns of the $2N \times 2N$ matrix

$$L = \begin{pmatrix} I & 0 \\ h & qI \end{pmatrix}.$$

Here h is a circulant matrix formed as a product $h \equiv pf^{-1}g \pmod{q}$, where f and g have small coordinates and p is small number with $\gcd(p, q) = 1$. We will also write f and g to denote the vectors formed by the first column of the corresponding matrix.

Private Key. The private key is the matrix f, which is used to form a $3N$ dimensional lattice generated by the rows of the matrix

$$L' = \begin{pmatrix} I & 0 & 0 \\ f & qI & 0 \\ I & qF & pI \end{pmatrix}.$$

(Here F is a circulant matrix related to f by the congruence $fF \equiv I \pmod{p}$.) Another way to think of this is to note that the vector $\begin{pmatrix} f \\ pg \end{pmatrix}$ is a small vector in the lattice L, so the private key is formed using a small vector in L.

Backdoor/Hard Problem. The key creator knows a short vector in the lattice L because he started with a short vector and used it to create the lattice. A potential codebreaker who wants to create her own decoding key needs to solve the hard problem of finding a short vector in the lattice L.

Encoded Message. An encoded message consists of a small perturbation of a random vector in the public lattice L. Mathematically, the encoded message is the vector e produced by

$$\begin{pmatrix} 0 \\ e \end{pmatrix} = \begin{pmatrix} I & 0 \\ h & qI \end{pmatrix} \begin{pmatrix} \phi \\ \psi \end{pmatrix} + \begin{pmatrix} -\phi \\ m \end{pmatrix}.$$

Here ϕ is a random (small) vector, ψ is chosen so that e has coordinates between 0 and $q - 1$, and m is the plaintext message whose coordinates are between 0 and $p - 1$.

Backdoor/Hard Problem. A potential codebreaker who wants to recover the message m directly needs to solve the hard problem of finding a vector in the lattice L which is very close to the known vector $\binom{0}{e}$. The key creator's backdoor is knowledge of a different lattice in which the "close vector" problem can be solved more easily.

Decoding a Message. To decode a message e, the decoder looks for a vector in the lattice L' which is close to the vector $\begin{pmatrix} e \\ 0 \\ 0 \end{pmatrix}$. This is done by computing

$$\begin{pmatrix} e \\ a \\ b \end{pmatrix} = \begin{pmatrix} I & 0 & 0 \\ f & qI & 0 \\ I & qF & pI \end{pmatrix} \begin{pmatrix} e \\ \lambda \\ \mu \end{pmatrix}$$

where λ and μ are chosen as follows. First, λ is chosen to make $fe + qI\lambda$ as small as possible. If the parameters have been chosen properly, this choice of λ will yield

$$a = fe + q\lambda = p\phi g + mf.$$

Then the decoder finds that b equals

$$\begin{aligned} b &= e + qF\lambda + p\mu \\ &= e + F(p\phi g + mf - fe) + p\mu \\ &= m + (fF - I)(m - e) + p\phi + p\mu. \end{aligned}$$

Note $fF \equiv I \pmod{p}$, so if the decoder chooses μ to make b as small as possible, he finds that $b = m$, thereby recovering the message.

References. Basic information about the RSA, McEliece, and El Gamel Public Key Cryptosystems can be found in any standard text on cryptography, such as *Cryptography: Theory and Practice*, D. Stinson, CRC Press, Boca Raton, 1995. The GGH PKCS is described in *Public-key cryptosystems from lattice reduction problems*, O. Goldreich, S. Goldwasser, S. Halevi, MIT – Laboratory for Computer Science preprint, November 1996.

Comments and questions concerning this technical report should be addressed to

`techsupport@ntru.com`

Additional information concerning NTRU Cryptosystems and the NTRU Public Key Cryptosystem are available at

`www.tiac.net/users/ntru`
