A Note on the Security of NTRUSign

Phong Q. Nguyen
École normale supérieure & CNRS, France
http://www.di.ens.fr/~pnguyen/

November 3, 2006

Abstract

At Eurocrypt '06, Nguyen and Regev presented a new key-recovery attack on the Goldreich-Goldwasser-Halevi (GGH) lattice-based signature scheme: when applied to NTRUSign-251 without perturbation, the attack recovers the secret key given only 90,000 signatures. At the rump session, Whyte speculated whether the number of required signatures might be significantly decreased to say 1,000, due to the special properties of NTRU lattices. This short note shows that this is indeed the case: it turns out that as few as 400 NTRUSign-251 signatures are sufficient in practice to recover the secret key. Hence, NTRUSign without perturbation should be considered totally insecure.
Keywords: NTRUSign, Parallelepiped.

1 Background

We assume the reader is familiar with the Nguyen-Regev paper [9] on attacking GGH [4] and NTRU [5] signatures: we follow the same notations as [9]. Vectors of $\mathbb{R}^n$ will be row vectors denoted by bold lowercase letters such as $\mathbf{b}$, and we will use row representation for matrices. The group of $n \times n$ invertible matrices with real coefficients will be denoted by $GL_n(\mathbb{R})$.

1.1 NTRUSign

NTRUSign [5] is a special instantiation of GGH [4] with the compact lattices from the NTRU encryption scheme [8], which we briefly recall: we refer to [5, 3] for more details. In the NTRU standards [3] which were being considered by IEEE P1363.1 [10], one selects $n = 251$ and $q = 128$. Let $\mathcal{R}$ be the ring $\mathbb{Z}[X]/(X^n - 1)$ whose multiplication is denoted by $*$. Using resultants, one computes a quadruplet $(f, g, F, G) \in \mathcal{R}^4$ such that $f * G - g * F = q$ in $\mathcal{R}$ and f is invertible mod q, where f and g have 0–1 coefficients (with a prescribed number of 1), while F and G have slightly larger coefficients, yet much smaller than q. This quadruplet is the NTRU secret key. It defines a lattice L, given by the secret basis formed by the rows of the following $(2n) \times (2n)$ matrix:

$$R = \begin{bmatrix} f_0 & f_1 & \cdots & f_{n-1} & g_0 & g_1 & \cdots & g_{n-1} \\ f_{n-1} & f_0 & \cdots & f_{n-2} & g_{n-1} & g_0 & \cdots & g_{n-2} \\ \vdots & \ddots & \ddots & \vdots & \vdots & \ddots & \ddots & \vdots \\ f_1 & \cdots & f_{n-1} & f_0 & g_1 & \cdots & g_{n-1} & g_0 \\ F_0 & F_1 & \cdots & F_{n-1} & G_0 & G_1 & \cdots & G_{n-1} \\ F_{n-1} & F_0 & \cdots & F_{n-2} & G_{n-1} & G_0 & \cdots & G_{n-2} \\ \vdots & \ddots & \ddots & \vdots & \vdots & \ddots & \ddots & \vdots \\ F_1 & \cdots & F_{n-1} & F_0 & G_1 & \cdots & G_{n-1} & G_0 \end{bmatrix},$$

where f_i denotes the coefficient of X^i of the polynomial f. Due to the special structure of R, it turns out that a single row of R is sufficient to recover the whole secret key. Because f is chosen invertible mod q, the polynomial $h = g/f \pmod q$ is well-defined in $\mathcal{R}$: this is the NTRU public key. Its fundamental property is that $f * h \equiv g \pmod q$ in $\mathcal{R}$. The polynomial h defines a natural public basis of L, which we omit (see [5]).

The messages are assumed to be hashed in $\{0, \ldots, q-1\}^{2n}$. Let $\mathbf{m} \in \{0, \ldots, q-1\}^{2n}$ be such a hash. We write $\mathbf{m} = (\mathbf{m}_1, \mathbf{m}_2)$ with $\mathbf{m}_i \in \{0, \ldots, q-1\}^n$. It is shown in [5] that the NTRU secret key (f, g, F, G) allows to compute a lattice vector $(\mathbf{s}, \mathbf{t}) \in \mathbb{Z}^{2n}$ which is rather close to $\mathbf{m}$: it is the output of the so-called Babai's rounding algorithm [1]. In practice, the signature is simply $\mathbf{s}$ and not $(\mathbf{s}, \mathbf{t})$, as $\mathbf{t}$ can be recovered from $\mathbf{s}$ thanks to $\mathbf{h}$. To verify the signature $\mathbf{s}$ of a message $\mathbf{m}$, one recovers $\mathbf{t}$ so that $(\mathbf{s}, \mathbf{t}) \in L$, and check that $(\mathbf{s}, \mathbf{t})$ is sufficiently close to $\mathbf{m}$.

This is the basic NTRUSign scheme [5] without perturbation. In order to strengthen the security of NTRUSign, perturbation techniques have been proposed in [6, 3, 7] and are now recommended. Roughly speaking, such techniques perturb the hashed message $\mathbf{m}$ before signing with the NTRU secret basis. However, there was no perturbation in half of the parameter choices recommended in NTRU standards [3] under consideration by IEEE P1363.1 at the time of writing of [9]. Namely, this was the case for the parameter choices `ees251sp2`, `ees251sp3`, `ees251sp4` and `ees251sp5` in [3]. For the other half, only a single perturbation was recommended.

1.2 The Parallelepiped Attack

In [9], it is shown that after many random pairs (message,signature) have been released, an attacker who wants to recover the secret key is faced with the following learning problem:

Problem 1.1 (The Hidden Parallelepiped Problem or HPP) *Let $V = [\mathbf{v}_1, \ldots, \mathbf{v}_m] \in GL_m(\mathbb{R})$. Define the parallelepiped spanned by V as $\mathcal{P}(V) = \{\sum_{i=1}^m x_i \mathbf{v}_i,\ x_i \in [-1, 1]\}$. Denote by $U(\mathcal{P})$ the uniform distribution on a parallelepiped $\mathcal{P}$. Given* poly(m) *samples from $U(\mathcal{P}(V))$, find a good approximation of the rows of $\pm V$.*

Here, $m = 2n$ where n is the NTRUSign parameter, and the matrix V is the NTRUSign secret key R previously described. Nguyen and Regev [9] further presented a statistical method based on a gradient descent to solve the HPP: it was reported that experimentally, in the case of NTRUSign-251, 90,000 pairs (message,signature) were sufficient to recover the secret key. Whyte noted in [12] that the figure of 90,000 was higher than the figure of 10,000 allowed by NTRU guidelines for the unperturbed case, and stated that "users who follow NTRU guidance would nevertheless be safe". However, [12] also recommended that more time be taken to study the attack before proceeding with standardization of NTRUSign. Whyte observed roughly one month later in [11] that NTRU bases have special properties which perhaps might lead to improved attacks: though no attack was presented in [11], NTRUSign without perturbation was no longer recommended. We now explain those special properties.

2 Symmetries in the NTRU Parallelepiped

2.1 Symmetries

Whyte [11] observed that in the particular case of NTRUSign, the hidden parallelepiped $\mathcal{P}(R)$ has a peculiar property: for each $\mathbf{x} \in \mathcal{P}(R)$, the block-rotation $\sigma(\mathbf{x})$ also belongs to $\mathcal{P}(R)$, where σ is

Table 1: New experiments on NTRUSign-251 without perturbation.

Number of signatures	Expected number of descents to recover the secret key
1,000	2
500	40
400	100

the application which maps any $(x_1, \ldots, x_n, y_1, \ldots, y_n) \in \mathbb{R}^{2n}$ to $(x_n, x_1, \ldots, x_{n-1}, y_n, y_1, \ldots, y_{n-1})$. This is because σ maps each row of the $(2n) \times (2n)$ matrix R to another of those rows. As a result, each sample in the parallelepiped $\mathcal{P}(R)$ actually gives rise to n samples in the parallelepiped $\mathcal{P}(R)$, thanks to the n rotations. Whyte concluded in [11] that the parallelepiped $\mathcal{P}(R)$ is uniquely determined after $O(q)$ signatures have been released, and left it as a challenge to attack NTRUSign without perturbations given only 1,000 signatures.

2.2 Exploiting the Symmetries

Here, we observe that Whyte's remark can be exploited by the attack of [9]: the attack remains the same, except that we derive n samples in the parallelepiped $\mathcal{P}(R)$ from each signature released, thanks to the block-rotation σ. For instance, 400 NTRUSign-251 signatures give rise to 100,400 samples in the NTRU parallelepiped. In doing so, we no longer have independent samples in the parallelepiped, but we can still run the attack and see if it works or not.

We experimented with the attack [9] on genuine NTRUSign-251 signatures of messages generated uniformly at random over $\{0, \ldots, q-1\}^{2n}$. Using the block-rotations, it seems that the number of signatures required by the attack becomes roughly divided by n, compared to [9]. Partial results are given in Table 1. As Table 1 shows, as few as 400 signatures are enough in practice to recover the secret key. Note that even the figure of 400 signatures may not be optimal.

2.3 Conclusion

In the particular case of NTRUSign, the number of signatures required for the key-recovery attack of [9] can significantly be reduced in practice, thanks to the symmetries of NTRU parallelepipeds. Namely, as few as 400 signatures are sufficient to break NTRUSign-251 without perturbation. Hence, NTRUSign without perturbation should be considered totally insecure.

References

[1] L. Babai. On Lovász lattice reduction and the nearest lattice point problem. *Combinatorica*, 6:1–13, 1986.

[2] ECCC. `http://www.eccc.uni-trier.de/eccc/`. The Electronic Colloquium on Computational Complexity.

[3] Consortium for Efficient Embedded Security. Efficient embedded security standards #1: Implementation aspects of NTRUEncrypt and NTRUSign. Version 2.0 available at [10], June 2003.

[4] O. Goldreich, S. Goldwasser, and S. Halevi. Public-key cryptosystems from lattice reduction problems. In *Proc. of Crypto '97*, volume 1294 of *LNCS*, pages 112–131. IACR, Springer-Verlag, 1997. Full version vailable at [2] as TR96-056.

[5] J. Hoffstein, N. A. Howgrave Graham, J. Pipher, J. H. Silverman, and W. Whyte. NTRUSIGN: Digital signatures using the NTRU lattice. Full version of [6]. Draft of April 2, 2002, available on NTRU's website.

[6] J. Hoffstein, N. A. Howgrave Graham, J. Pipher, J. H. Silverman, and W. Whyte. NTRUSIGN: Digital signatures using the NTRU lattice. In *Proc. of CT-RSA*, volume 2612 of *LNCS*, pages 122–140. Springer-Verlag, 2003.

[7] J. Hoffstein, N. A. Howgrave Graham, J. Pipher, J. H. Silverman, and W. Whyte. Performances improvements and a baseline parameter generation algorithm for NTRUsign. In *Proc. of Workshop on Mathematical Problems and Techniques in Cryptology*, pages 99–126. CRM, 2005.

[8] J. Hoffstein, J. Pipher, and J.H. Silverman. NTRU: a ring based public key cryptosystem. In *Proc. of ANTS III*, volume 1423 of *LNCS*, pages 267–288. Springer-Verlag, 1998. First presented at the rump session of Crypto '96.

[9] P. Q. Nguyen and O. Regev. Learning a parallelepiped: Cryptanalysis of GGH and NTRU signatures. In *Proc. of Eurocrypt '06*, volume 4004 of *LNCS*, pages 215–233. IACR, Springer-Verlag, 2006.

[10] IEEE P1363.1. Public-key cryptographic techniques based on hard problems over lattices. See `http://grouper.ieee.org/groups/1363/lattPK/index.html`, June 2003.

[11] W. Whyte. Improved NTRUSign transcript analysis. Presentation at the rump session of Eurocrypt '06, on May 30, 2006.

[12] W. Whyte. NTRUSign and P1363.1. Slides of April 11, 2006 available at `http://grouper.ieee.org/groups/1363/WorkingGroup/presentations/P1363.1-2006-04.ppt`, presenting the implications of [9] for IEEE P1363.1.