Peer Review and Independent Scrutiny

of the NTRUEncrypt Public Key Cryptosystem

Executive Summary

This document surveys the results of peer review of the NTRUEncrypt cryptosystem. The credibility and acceptance of any cryptosystem depends on the quality of the independent scrutiny it has received. NTRU Cryptosystems has always tried to encourage independent scrutiny of its algorithms, and to make this scrutiny as easy as possible. Our algorithms are published in peer-reviewed forums, our website contains a large amount of tutorial information (http://www.ntru.com/technology/tech.learning.htm), we have organized challenge problems to motivate scrutiny from the broader community, and we will always make a good-faith effort to ensure that all the relevant technical information is available to any researcher who is interested in our technology.

This effort on our part has been repaid by a tremendous amount of independent scrutiny, which this document summarizes.

The scrutiny confirms that the core technologies of NTRUEncrypt, NTRUSign, and the NTRU lattice are secure. No attack has been found which significantly impacts the core ideas in NTRU technology. When used with the correct parameters and correct message pre- and post-processing, the NTRU algorithms give the same level of data protection as other accepted public-key algorithms, such as RSA or ECC. The best current research affirms that NTRU makes it possible to have strong public-key cryptography at a fraction of the time and processing power previously necessary.

The rest of this document is organized into four sections: first, a history and overview of the peer review of the NTRUEncrypt Public Key Cryptosystem; second, a summary of published results on NTRUEncrypt; third, a bibliography of (selected) relevant references; fourth, an overview of the history of the NSS signing algorithm; and finally an appendix containing a brief overview of lattices and cryptography.

1. History and Overview of Peer Review of The NTRUEncrypt Public Key Cryptosystem

The NTRUEncrypt Public Key Cryptosystem was developed over a period of several years in the mid-1990s by a team of mathematicians (Jeffrey Hoffstein, Jill Pipher and Joseph Silverman – the same Joseph Silverman famous for his work on elliptic curves). Dr. Hoffstein first publicly presented the NTRUEncrypt algorithm, then simply called "NTRU", at the rump session of CRYPTO 96. The team distributed a preprint giving a full description of the algorithm and a preliminary security analysis, and also made it available via the NTRU Cryptosystems website.

Over the next two years, numerous comments from leading cryptographers, including Don Coppersmith, Johan Håstad, Andrew Odlyzko, and Adi Shamir, helped to refine the security analysis. This did not lead to any changes in the underlying NTRU algorithm, but did suggest the use of somewhat larger parameters to achieve the desired security levels. (This is exactly analogous to the way in which new factoring methods have led to the use of larger primes in RSA, without in any way affecting the underlying RSA encryption algorithm.) The full NTRU algorithm and security analysis was then published in the proceedings of the Algorithmic Number Theory Symposium (ANTS III, Portland 1998), resulting in further scrutiny.

Before proceeding to describe this scrutiny, we make a few observations.

1) The use of the word "attack" is not the same in cryptographic papers as it is in common English usage. In a cryptographic paper, "attack" does not mean "total break". It may apply only to a particular parameter set or padding scheme for the cryptosystem, and an attack may enable an attacker to recover a small amount of information about a single message, or to recover the entire encrypted message, or to recover keying material. Additionally, an attack may simply be an analysis of approaches to attacking a system; an attack need not be practical to be published, so long as it contains an interesting insight. **The word "attack" in the title of a paper does not mean the target system is broken**.
2) A public-key cryptosystem typically consists of a core hard mathematical problem, recommended parameter sets defining an instance of the hard problem, and recommended message processing to be performed on encryption or decryption. An "attack" can be an observation about any one or more of these components. For example, the analysis in Nguyen and Pointcheval's "Analysis and Improvements of NTRU Encryption paddings" (Crypto 2002) concerns only some of the message processing (or "padding") schemes proposed for NTRUEncrypt.
3) The name of a paper is no indication of whether it contains a crippling attack, or simply an interesting observation. One paper by Boneh, Joux and Nguyen at ASIACRYPT 2000 is entitled "Why Textbook ElGamal and RSA Encryption are Insecure." This does not mean that all implementations of RSA are insecure. Instead, the paper shows

that RSA can be implemented in a way that is vulnerable to certain classes of attacks, and outlines ways of avoiding these attacks.

We now survey peer review of NTRU.

The first paper studying NTRU technology was written by Don Coppersmith and Adi Shamir, two of the world's leading cryptographers. In that paper ("Lattice attacks on NTRU", really an *analysis* of lattice attacks on NTRU), they noted that the best way to attack the NTRU cryptosystem was via the techniques of lattice reduction and proposed and studied one such attack. This is completely analogous to noting that the best way to attack RSA is via factoring the modulus (or that the best way to attack ECC is via the Pollard rho method), and that different-size keys give different levels of security. The analysis in the paper contributes to establishing the appropriate key length for a desired security level.

More importantly, Coppersmith and Shamir's paper established NTRUEncrypt as a legitimate, interesting cryptosystem of academic as well as practical interest. This encouraged other researchers to turn their attention to the NTRU cryptosystem. In particular, experts in lattice reduction studied whether any of their specialized techniques could crack NTRUEncrypt. To date, this has not resulted in any published results that make use of unique properties of the NTRU lattice to speed up attacks: the best known attacks on the NTRU lattice are also the best known attacks on generic random lattices. No research to date has significantly impacted the perceived security of NTRU lattice parameters.

The remaining issues are the recommended parameter sets and the appropriate padding scheme for use on encryption and decryption.

Here there has also been intensive research. Jaulmes and Joux demonstrated in 2000 that care must be taken in the choice of padding scheme to prevent adaptive chosen ciphertext attacks, and that part of this defense must be an assurance that the values m and r are chosen as directed by the parameter sets. More recent results (by Howgrave-Graham *et al*, Proos, and others) have shown that the parameter sets must be chosen to keep decryption failures to a negligible level. Once the correct parameter sets and padding scheme have been chosen, however, it can be shown that any successful attack on NTRUEncrypt must be an attack on the underlying hard lattice problem.

So just as RSA is secure – unless there is a new breakthrough in factoring, and ECC is secure – unless there is a new breakthrough in elliptic curve discrete logarithm techniques, the NTRU cryptosystem is also secure – unless there is a new breakthrough in lattice reduction. In each of these three cases, no breakthrough is on the horizon.

There have been many other papers studying NTRUEncrypt, and it has become a standard topic for cryptography courses and seminars throughout the world. In addition, the NTRU cryptosystem is featured in recent cryptography textbooks such as Paul Garrett's Making,

Breaking Codes: An Introduction to Cryptology (Prentice-Hall, 2001). Stern and Nguyen, two leading experts in the application of lattice techniques to cryptography, concluded in 2001 that NTRUEncrypt "the leading candidate among knapsack-based and lattice-based cryptosystems."

The NTRUSign cryptosystem is more recent, and has not received the same amount of direct scrutiny as NTRUEncrypt. However, it makes use of the same underlying lattice problem, and as such all of the research on the core NTRUEncrypt lattice problem also affirms the security of NTRUSign. The major research result on NTRUSign is due to Gentry and Szydlo, who observed that a transcript of signatures leaks information about the private key and estimated the transcript length necessary to recover the private key. This attack is countered by the use of perturbations in NTRUSign signatures, which allow a signer to make the required transcript almost arbitrarily long with very little loss of efficiency. No significant attack on NTRUSign with perturbations has ever been demonstrated.

2. Scrutiny of the NTRU Cryptosystem

Cryptographers around the world continue their studies of the NTRU cryptosystem. This section reviews the significant papers about NTRUEncrypt and NTRUSign. The papers are reviewed in order of publication, most recent first. In this section, we assume some familiarity with NTRU terminology.

N. Howgrave-Graham, J. Hoffstein, J. Pipher, W. Whyte, On Estimating the Lattice Security of NTRU, available from http://www.ntru.com/cryptolab/articles.htm#2005_2.

> The paper analyzes the claims of Buchmann and Ludwig below and disputes their results.
>
> First, Schnorr fourth-roots the time for Koy's primal-dual method, not the time for BKZ with a certain blocksize, so it is not valid to draw a link between BKZ times and times achieved by their method in the absence of experimental evidence. Second, their claim that their method 3/4-roots running times is unjustified. Third, Schnorr's result is asymptotic and it is not clear that, even if it reduced the time for BKZ, this effect would be noticeable at the moderate dimensions under consideration.
>
> Finally, we explicitly analyze the expected running times of Schnorr's method, applied to the NTRU lattice. In the special case of binary *f*, Schnorr's algorithm essentially reduces to brute force search with running time about 2^N. In the more general case, we expect the running time of a naïve application of Schnorr's algorithm to be superexponential. Since the Ludwig/Buchmann algorithm is admitted to be less efficient in general than Schnorr's algorithm, we consider it unlikely that it impacts the security of the current NTRU parameter sets.

J. Buchmann, C. Ludwig, Practical Lattice Basis Sampling Reduction, available from http://eprint.iacr.org/2005/072.

> The paper proposes a practical sampling reduction algorithm for lattice bases based on work by Schnorr as well as two even more effective generalizations. It reports the empirical behaviour of these algorithms. It describes how Sampling Reduction allows to stage lattice attacks against the NTRU cryptosystem with smaller BKZ parameters than before and claims that therefore the recommended NTRU security parameters offer <= 74 Bit security.

S. Min, G. Yamamoto, K. Kim, Weak property of malleability in NTRUSign, ACISP04, July 13-15, Sydney, Australia

> The paper demonstrates a weak property of malleability in NTRUSign: given a signature *s* on a specific message, a forger can generate *q*-1 additional signatures on the same

message. This shows that NTRUSign as specified falls short of the very strongest notion of security for signatures, although there are few situations in which this makes any practical difference. The paper also proposes a simple and efficient fix. The paper does not demonstrate a means for forging on other, unsigned messages.

N. Howgrave-Graham, J. Silverman, A. Singer, W. Whyte, NAEP: Provable security in the presence of decryption failures. Available from http://www.ntru.com/cryptolab/articles.htm#006.

The paper presents a padding scheme appropriate for cryptosystems with a non-zero but negligible average-case chance of decryption failure. It explains the application of this padding scheme to NTRUEncrypt and gives a proof of security. This is the first full proof of security for NTRUEncrypt, demonstrating that the problem of breaking NTRUEncrypt reduces to the problem of finding a close vector in a specific lattice.

N. Howgrave-Graham, J.H. Silverman, W. Whyte, A meet-in-the-middle attack on an NTRU private key, NTRU Technical Report 004, version 2, 2003. Available from http://www.ntru.com/cryptolab/tech_notes.htm#004.

This note describes a technique, originally due to Odlyzko, for trading off memory for time in searching for an NTRUEncrypt private key by a brute-force method. It demonstrates that for recommended parameter sets with N=251 the strength against meet-in-the-middle attacks is at least 2^{80}.

J. Hoffstein, J. Silverman, W. Whyte, NTRU Technical Report #12, v2, Estimating Breaking Times for NTRU Lattices. Available from http://www.ntru.com/cryptolab/tech_notes.htm#012.

The paper discusses the best known lattice-based attacks on NTRU cryptosystems, and demonstrates that for recommended parameter sets with N=251 the strength against lattice attacks is at least 2^{80}.

J. Silverman, W. Whyte, NTRU Technical Report #18, Estimating Decryption Failure Probabilities for NTRUEncrypt. Available from http://www.ntru.com/cryptolab/tech_notes.htm#018.

The paper discusses how to analyze the probability of an NTRUEncrypt decryption failure, and demonstrates that there are parameter sets which reduce the probability of a decryption failure to less than 2^{-80} for N=251.

N. Howgrave-Graham, P. Nguyen, D. Pointcheval, J. Proos, J. Silverman, A. Singer, W. Whyte, The Impact of Decryption Failures on the Security of NTRU Encryption. Available from http://www.ntru.com/cryptolab/articles.htm#005. Proc. Crypto 2003, to appear.

The paper describes an attack on NTRU as described in EESS#1 with the SVES-1 or SVES-2 padding scheme. The attack uses decryption failures to recover the private key with about 2^{40} queries to a decryption oracle. It illustrates the importance of choosing parameter sets such that the chance of decryption failures is negligible.

M. Szydlo, Hypercubic Lattice Reduction and Analysis of GGH and NTRU Signatures, *EUROCRYPT 2003*, Warsaw, Poland, 2003, Lect. Notes in Comp. Sci., Springer-Verlag, Berlin, 2003, v.2656, 433-448. Available from http://www.szydlo.net.

The paper considers a problem that arises naturally in the context of NTRUSign signature transcript analysis, the *Gram Matrix Problem* of recovering a unitary matrix U from its Gram matrix $G = UU^T$. It shows this is polynomial-time equivalent to a problem which is conjectured to be simpler. This result does not affect the advertised security of NTRUSign, as the advertised security of NTRUSign does not depend on that the Gram Matrix problem is hard (and, in fact, assumes that it is easy).

M. Naslund, I. Shparlinski, W. Whyte, On the Bit Security of NTRUEncrypt, *Proc. Intern. Workshop on Public Key Cryptography, PKC'03*, Miami, USA, 2003, Lect. Notes in Comp. Sci., Springer-Verlag, Berlin, 2003, v.2567, 62-70. Available from http://www.ntru.com/cryptolab/articles.htm#004.

The paper shows that in certain natural computational models every bit of a message encrypted with NTRUEncrypt is as secure as the whole message.

T. Meskanen, A. Renvall, A Wrap Error Attack Against NTRUEncrypt, University of Turku Technical Report TUCS 507. Available from http://www.tucs.fi/Research/Series/techreports/techrep.php?year=2003. Presented at WCC 2003.

The paper describes an attack on NTRUEncrypt as described in EESS#1 with the SVES-1 padding scheme. The attack uses decryption failures to recover the private key, exploiting the fact that the chosen parameter sets do not constrain r to be binary.

J. Proos, Imperfect Decryption and an Attack on the NTRU Encryption Scheme. Available from http://eprint.iacr.org/2003/002/.

The paper describes an attack on NTRUEncrypt as described in early NTRU Cryptosystems, Inc papers with p=3 and different padding schemes. The attack uses decryption failures to reduce the size of the lattice problem that must be solved to recover the private key. The attack is successful with relatively few messages, emphasizing the importance of choosing the correct padding scheme and a parameter set that reduces the chance of decryption failures.

J. Hong, J. W. Han, D. Kwon, D. Han, Key Recovery Attacks on NTRU without Ciphertext Validation Routine. Available from http://eprint.iacr.org/2002/188/. Accepted for publication at ACISP 2003. Originally named Chosen-Ciphertext Attacks on Optimized NTRU.

> The paper describes an attack on NTRUEncrypt without the use of a specially designed padding scheme. The paper illustrates the importance of choosing the correct padding scheme for a public-key encryption algorithm such as NTRUEncrypt.

P. Nguyen, D. Pointcheval, Analysis and Improvements of NTRU Encryption Paddings, *Proc. CRYPTO 2002*, Lecture Notes in Computer Science, Springer-Verlag 2002. Available from http://www.di.ens.fr/~pointche/pub.php?reference=NgPo02.

> The paper analyses the security against chosen plaintext attack given by three different padding schemes proposed for NTRUEncrypt. It demonstrates that care must be taking when adding random data to a message to ensure that the random data gives full protection against brute-force distinguishing attacks.

C. Gentry, M. Szydlo, Cryptanalysis of the revised NTRU Signature Scheme, *Proc. EUROCRYPT 2002*, Lecture Notes in Computer Science, Springer-Verlag, 2002

> The paper demonstrated that the (now abandoned) NSS algorithm was insecure. It also showed how an attacker could recover information from a transcript of signatures generated by the NTRUSign algorithm. The use of perturbations, as recommended in the NTRUSign paper presented at CT-RSA 2003, can essentially eliminate the information leakage from transcripts.

C. Gentry, Key Recovery and Message Attacks on NTRU-Composite, *Proc. EUROCRYPT 2001*, Lecture Notes in Computer Science, Springer-Verlag, 2001

> The paper presents a clever attack that would work against NTRUEncrypt if NTRUEncrypt were ever deployed with the security parameter N not a prime number. In practice, NTRU Cryptosystems has strongly recommended that N always be prime. Indeed, all commercial implementations conform to NTRU's recommendations, and are immune to this attack.

P. Nguyen, J. Stern, Lattice Reduction in Cryptology: An Update, *Cryptography and Lattices Conference (CaLC 2001)*, Lecture Notes in Computer Science 2146, Springer-Verlag, 2001

The paper surveys the use of lattices in both making and breaking cryptosystems. NTRUEncrypt (then known simply as NTRU) is considered "the leading candidate among knapsack-based and lattice-based cryptosystems."

É. Jaulmes, A. Joux, A chosen-ciphertext attack against NTRU, *Advances in Cryptology-CRYPTO 2000*, Lecture Notes in Computer Science, Springer-Verlag, 2000

Chosen-ciphertext attacks exist for all public key cryptosystems, including RSA, ECC and NTRUEncrypt. Such attacks may be possible even if the underlying hard mathematical problem is secure. They typically rely on sending specially constructed fake messages to a decryptor and watching to see what happens. If the underlying cryptographic primitive is secure, a well-chosen padding scheme will typically prevent chosen ciphertext attacks. The Jaulmes-Joux paper presents an interesting chosen-ciphertext attack against NTRUEncrypt with the padding schemes that were recommended at the time; the recommended padding schemes have since been altered.

A. May, J.H. Silverman, Dimension reduction methods for convolution modular lattices, Cryptography and Lattices Conference (CaLC 2001), Lecture Notes in Computer Science 2146, Springer-Verlag, 2001
J.H. Silverman, Dimension reduced lattices, zero-forced lattices, and the NTRU public key cryptosystem, NTRU Technical Report 013, 1999, www.ntru.com

NTRU private keys consist of known numbers of 0s and 1s. These papers describe a means of exploiting this fact to speed up attacks. For commercial-grade NTRU, the speed gain does not have a significant impact on the security of the algorithm (attacks are speeded up by a factor of, typically, 10 to 20).

J. Hoffstein, J.H. Silverman, Implementation Notes for NTRU PKCS Multiple Transmissions, NTRU Technical Report 06, 1998, see http://www.ntru.com/technology/techpapers/tech.technical.abstracts.htm.

This technical note comments on a simple "gotcha" when performing NTRU encryption and decryption: it is inadvisable to use the same blinding value twice, or to encrypt the same message twice with different blinding values. The use of Fujisaki-Okamoto message processing, as recommended by NTRU and provided in all NTRU products, means that the second of these will never happen, and makes the first vanishingly unlikely.

J.H. Silverman, A meet-in-the-middle attack on an NTRU private key, NTRU Technical Report 004, 1997, see http://www.ntru.com/technology/techpapers/tech.technical.abstracts.htm.

This note describes a technique, originally due to Odlyzko, for trading off memory for time in searching for an NTRUEncrypt private key by a brute-force method. However,

lattice-based attacks on NTRUEncrypt are still more effective than brute-force searches, even when this technique is used.

D. Coppersmith, A. Shamir, Lattice attacks on NTRU, in *Proc. of EUROCRYPT 97*, Lecture Notes in Computer Science, Springer-Verlag, 1997 [CS97].

The paper notes that the best way to attack NTRUEncrypt is via the techniques of lattice reduction and describes one such attack. This is analogous to noting that the best way to attack RSA is via factoring the modulus (or that the best way to attack ECC is via the Pollard rho method), and the defense is also completely analogous – one just uses parameter choices that make such attacks infeasible.

3. Bibliography

NTRU Research Articles

D. Coppersmith, A. Shamir, Lattice attacks on NTRU, *Advances in Cryptology — Eurocrypt '97*, Lecture Notes in Computer Science 1233, Springer-Verlag, 1997, 52-61.

P. Garrett, *Making, Breaking Codes: An Introduction to Cryptology*, Prentice-Hall, 2001. [NTRU is covered in Section 10.6 of this standard textbook.]

C. Gentry, Key Recovery and Message Attacks on NTRU-Composite, *Advances in Cryptology — Eurocrypt 2001*, Lecture Notes in Computer Science 2045, Springer-Verlag,, 2001

C. Gentry, J. Jonsson, M. Szydlo, J. Stern, Cryptanalysis of the NTRU Signature Scheme (NSS) from Eurocrypt 2001, *Advances in Cryptology – AsiaCrypt 2001*, Lecture Notes in Computer Science, Springer-Verlag, to appear.

C. Gentry, M. Szydlo, Cryptanalysis of the Revised NTRU Signature Scheme, *Advances in Cryptology – Eurocrypt 2002*, Springer-Verlag, 2002, 299-320.

J. Hoffstein, J. Pipher, J. Silverman, NTRU: A Ring Based Public Key Cryptosystem, *Algorithmic Number Theory (ANTS III)*, Portland, OR, June 1998, J.P. Buhler (ed.), Lecture Notes in Computer Science 1423, Springer-Verlag, Berlin, 1998, 267-288.

J. Hoffstein, J. Pipher, J. Silverman, NSS: An NTRU Lattice-Based Signature Scheme, *Advances in Cryptology — Eurocrypt 2001*, Lecture Notes in Computer Science 2045, Springer-Verlag,, 2001

J. Hoffstein, J. Pipher, J. Silverman, *The NTRU Signature Scheme: Theory and Practice*, available at http://www.ntru.com/technology/tech.technical.htm.

J. Hoffstein, D. Lieman, J. Silverman, Polynomial Rings and Efficient Public Key Authentication, *Proceeding of the International Workshop on Cryptographic Techniques and E-Commerce (CrypTEC '99)*, M. Blum and C.H. Lee, eds., City University of Hong Kong Press, to appear.

J. Hoffstein, J. Silverman, Polynomial Rings and Efficient Public Key Authentication II, *Proceedings of a Conference on Cryptography and Computational Number Theory (CCNT '99)*, I. Shparlinski et.al., eds., Birkhauser, 269-286.

J. Hoffstein, J. Silverman, MiniPASS: Authentication and Digital Signatures in a Constrained Environment, *Cryptographic Hardware and Embedded Systems-CHES 2000*, C.K. Koc and C. Paar, eds., Lecture Notes in Computer Science 1965, Springer-Verlag, 2000, 328-339.

J. Hoffstein, J. Silverman, Optimizations for NTRU, *Public-Key Cryptography and Computational Number Theory* (Warsaw, September 11-15, 2000), Springer-Verlag, to appear.

J. Hong, J. W. Han, D. Kwon, D. Han, Chosen-Ciphertext Attacks on Optimized NTRU, available from http://eprint.iacr.org/2002/188/.

N. Howgrave-Graham, P. Nguyen, D. Pointcheval, J. Proos, A. Singer, W. Whyte, The Impact of Decryption Failures on the Security of NTRU Encryption, available from http://www.ntru.com/cryptolab/articles.htm

N. Howgrave-Graham, J. Silverman, A. Singer, W. Whyte, Decryption Failures and Provability: SAEP+, NAEP and NTRU, available from http://www.ntru.com/cryptolab/articles.htm

E. Jaulmes and A. Joux, A chosen-ciphertext attack against NTRU, *Advances in Cryptology — CRYPTO 2000*, Lecture Notes in Computer Science, Springer-Verlag, to appear (August, 2000).

P. Karu and J. Loikkanen, Practical comparison of fast public-key cryptosystems, Seminar on Network Security, Telecommunications Software and Multimedia Laboratory, Helsinki University of Technology. (http://www.tml.hut.fi/Opinnot/Tik-110.501/2000/papers.html.)

A. May, J.H. Silverman, Dimension reduction methods for convolution modular lattices, *Conference on Lattices and Cryptography (CaLC 2001)*, Lecture Notes in Computer Science 2146, Springer-Verlag, 111-127.

A. May, *Auf Polynomgleichungen basierende Public-Key-Kryptosysteme*, Johann Wolfgange Goethe-Universitat, Frankfurt am Main, Fachbereich Informatik. (Masters Thesis in Computer Science, 4 June, 1999; Thesis advisor, Dr. C.P. Schnorr) Available at: www.mi.informatik.uni-frankfurt.de/research/mastertheses.html

T. Meskanen, A. Renvall, A Wrap Error Attack Against NTRUEncrypt, University of Turku Technical Report TUCS 507, available from http://www.tucs.fi/Research/Series/techreports/techrep.php?year=2003

S. Min, G. Yamamoto, K. Kim, Weak property of malleability in NTRUSign, ACISP04, July 13-15, Sydney, Australia, 2004.

S. Min, G. Yamamoto, K. Kim, On the security of NTRUSign signature scheme, SCIS 2004, The 2004 Symposium on Cryptography and Information Security, Sendai, Japan, 2004.

I. Mironov, A Note on Cryptanalysis of the Preliminary Version of the NTRU Signature Scheme, Cryptology ePrint Archive 2001/005 (available at http://eprint.iacr.org).

P. Nguyen, D. Pointcheval, Analysis and Improvements of NTRU Encryption Paddings, *Proc. CRYPTO 2002*, Lecture Notes in Computer Science, Springer-Verlag 2002.

P. Nguyen, J. Stern, Lattice Reduction in Cryptology: An Update, *Conference on Lattices and Cryptography (CaLC 2001)*, Lecture Notes in Computer Science 2146, Springer-Verlag

J. Proos, Imperfect Decryption and an Attack on the NTRU Encryption Scheme, available from http://eprint.iacr.org/2003/002/.

J. Silverman, W. Whyte, Estimating Decryption Failure Probabilities for NTRUEncrypt, available from http://www.ntru.com/cryptolab/articles.htm

NTRU Cryptosystems Technical Notes

These are available from http://www.ntru.com/cryptolab/tech_notes.htm.

#004 A Meet-In-The-Middle Attack on an NTRU Private Key
#005 Hard Problems and Backdoors for NTRU and Other PKCS's
#006 Implementation Notes for NTRU PKCS Multiple Transmissions
#007 Plaintext Awareness and the NTRU PKCS
#008 Efficient Conversions from Mod q to Mod p
#009 Invertibility in Truncated Polynomial Rings
#010 High-Speed Multiplication of (Truncated) Polynomials
#011 Wraps, Gaps, and Lattice Constants
#012 Estimated Breaking Times for NTRU Lattices
#013 Dimension-Reduced Lattices, Zero-Forced Lattices, and the NTRU Public Key Cryptosystem
#014 Almost Inverses and Fast NTRU Key Creation
#015 Reaction Attacks Against the NTRU Public Key Cryptosystem
#016 Protecting NTRU Against Chosen Ciphertext and Reaction Attacks
#018 Estimating Decryption Failure Probabilities for NTRUEncrypt

Some Representative Articles on Lattices and Cryptography

M. Ajtai, C. Dwork, A public-key cryptosystem with worst case/average case equivalence. *Proc. 29th ACM Symposium on Theory of Computing*, 1997, 284-293.

J. Blömer, J.-P. Seifert, On the Complexity of Computing Short Linearly Independent Vectors and Short Bases in a Lattice, *STOC '99*

J.Y. Cai, A.P. Nerukar, An improved worst-case to average-case reduction for lattice problems, *Proc. 38th Symposium on Foundations of Computer Science*, 1997, 468-477

I. Dinur, G. Kindler, S. Safra, Approximating CVP to within almost-polynomial factors is NP-hard, *Proc. 39th Symposium on Foundations of Computer Science*, 1998, 99-109

O. Goldreich, S. Goldwasser, On the limits of non-approximability of lattice problems, *Proc. 39th Symposium on Foundations of Computer Science*, 1998, 1-9

O. Goldreich, S. Goldwasser, S. Halvei, Public-key cryptography from lattice reduction problems. *Advances in Cryptology – CRYPTO '97*, Lecture Notes in Computer Science 1294, Springer-Verlag, 1997, 112-131.

O. Goldreich, D. Micciancio, S. Safra, J.-P. Seifert, Approximating shortest lattice vectors is not harder than approximating closest lattice vectors, *Electronic Colloquium on Computational Complexity*, TR99-002, 1999

C.J. Lagarias, H.W. Lenstra, C.-P. Schnorr, Korkin-Zolotarev bases and successive minima of a lattice and its reciprocal lattice, *Combitorica* 10 (1990), 333-348

A.K. Lenstra, H.W. Lenstra Jr., L. Lovász, Factoring polynomials with rational coefficients, *Mathematische Ann.* 261 (1982), 513-534.

R. Merkle, M. Hellman, Hiding information and signatures in trapdoor knapsacks, *IEEE Trans. Inform. Theory*, IT-24:525-530, September 1978.

D. Miociancio, The shortest vector in a lattice is hard to approximate to within some constant, *Proc. 39th Symposium on Foundations of Computer Science,* 1998, 92-98.

P. Nguyen, Cryptanalysis of the Goldreich-Goldwasser-Halevi Cryptosystem from Crypto '97, *Advances in Cryptology – CRYPTO '99*, Lecture Notes in Computer Science, Springer-Verlag.

C.-P. Schnorr, A hierarchy of polynomial time lattice basis reduction algorithms, *Theoretical Computer Science* 53 (1987), 201-224.

C.-P. Schnorr, A more efficient algorithm for lattice basis reduction, *J. Algorithms* 9 (1988), 47-62.

C.-P. Schnorr, M. Euchner, Lattice basis reduction: improved practical algorithms and solving subset sum problems, *Math. Programming* 66 (1994), no. 2, Ser. A, 181-199.

A. Shamir, A polynomial-time algorithm for breaking the basic Merkel-Hellman cryptosystem. *Proceedings of the 23rd IEEE Symposium on Foundations of Computer Science*, IEEE, 1982, 145-152.

4. The NSS Signature Algorithm

The NSS signature algorithm was proposed at the rump session of Crypto 2000, and broken (following a series of other results) by Gentry and Szydlo at the rump session of Crypto 2001.

None of the attacks on NSS compromised the security of NTRUEncrypt, or of the principles underlying NTRUEncrypt. Indeed, many of the attacks were primarily based on observations of how the NSS algorithm differed from NTRUEncrypt:

- In an early version of the NSS algorithm, the private key polynomials had some coefficients that were much larger than the average. This fact, and an attack based on it, were noted independently by Mironov and the NTRU research team. The attack does not apply to NTRUEncrypt or NTRUSign. In these algorithms, the secret polynomials have very little structure, and their coefficients lie within a narrow range.
- The NSS algorithm relied for security on the fact that some coefficients of the signature polynomial had been reduced modulo the parameter q. However, the signature polynomial was the product of two small polynomials, and because of this it was possible for an attacker to detect which coefficients had been reduced and correct for this reduction, "lifting" the polynomial to the space of the integers and halving the effective size of the lattice. This attack does not apply to NTRUEncrypt. Although NTRUEncrypt relies for its security on the fact that the coefficients of the ciphertext have been reduced modulo q, the ciphertext is the product of one small polynomial and one (statistically) random one. This means that almost all coefficients will naturally be reduced mod q, and there appears to be no way for an attacker to lift in this case.
- In the version of the NSS algorithm that appears in the Eurocrypt proceedings, the verification tests did not check tightly enough that the signature was bound to the correct message. There is no analogy between this and any possible attack on NTRUEncrypt.

Of the papers listed above, the following relate only to the NSS algorithm:

NSS Research Articles

C. Gentry, J. Jonsson, M. Szydlo, J. Stern, Cryptanalysis of the NTRU Signature Scheme (NSS) from Eurocrypt 2001, *Advances in Cryptology – AsiaCrypt 2001*, Lecture Notes in Computer Science, Springer-Verlag, to appear.

C. Gentry, M. Szydlo, Cryptanalysis of the Revised NTRU Signature Scheme, *Advances in Cryptology – Eurocrypt 2002*, Springer-Verlag, 2002, 299-320.

J. Hoffstein, J. Pipher, J. Silverman, NSS: An NTRU Lattice-Based Signature Scheme, *Advances in Cryptology — Eurocrypt 2001*, Lecture Notes in Computer Science 2045, Springer-Verlag, 2001

J. Hoffstein, J. Pipher, J. Silverman, *The NTRU Signature Scheme: Theory and Practice*, available at http://www.ntru.com/technology/tech.technical.htm.

I. Mironov, A Note on Cryptanalysis of the Preliminary Version of the NTRU Signature Scheme, Cryptology ePrint Archive 2001/005 (available at http://eprint.iacr.org).

NTRU Cryptosystems Technical Notes concerning NSS

#017 Enhanced Encoding and Verification Methods for the NTRU Signature Scheme

Appendix: Lattices and Cryptography

Lattices and Hard Lattice Problems

The hard problem underlying the NTRUEncrypt Cryptosystem is the problem of finding short vectors (SVP) or close vectors (CVP) in a lattice. Although it has not been proven that breaking NTRU is equivalent to solving this problem in a random lattice, the most effective known attacks on NTRU involve solving an SVP or a CVP without taking the precise structure of the lattice into account. (This is analogous to the fact that although breaking RSA has not been proven to be equivalent to factoring, the most effective known attacks involve factoring.)

A *lattice* L of dimension N is a collection of vectors

$a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + \ldots + a_N\mathbf{v}_N$ for all integers $a_1,a_2,\ldots,a_N$

where $\mathbf{v}_1,\mathbf{v}_2,\ldots,\mathbf{v}_N$ is a basis of vectors for $\mathbf{R}^N$. Cryptography uses lattices having integer coordinates.

- The *Shortest Vector Problem* (SVP) in L is the problem of finding the shortest nonzero vector in L.
- The *Closest Vector Problem* (CVP) in L is the problem of finding the vector in L that is closest to a given vector $\mathbf{w}$ in $\mathbf{R}^N$. In full generality, the CVP is NP-complete.

Two early important results in the theory of lattices are:

- **Hermite's Theorem** (ca. 1880) – Gives an upper bound for the shortest nonzero vector in a lattice in terms of the dimension and the covolume of the lattice.
- **Minkowski's Convex Body Theorem** (1896) – A convex symmetric set in $\mathbf{R}^N$ with volume larger than 2^NCovolume(L) contains a nonzero lattice vector.

Lattices and the Geometry of Numbers

- Lattices and the key problems (SVP and CVP) have been the subject of intense mathematical investigation for over 100 years.
- Minkowski named this subject the **Geometry of Numbers**. (*Geometrie der Zahlen*, Leipzig, 1910.)
- The "bible" is Lekkerkerker's *Geometry of Numbers* (1969)—510 pages long with a 32 page bibliography. When Lekkerkerker was updated (2^{nd} edition, 1987), it grew to 732 pages with a 93 page bibliography.
- There were more than 14,000 articles published between 1986 and 1999 with the word "Lattice" in their title.
- Not all research on lattices is directly relevant to cryptography; there is no question that lattices are a fundamental object of study in algebra, geometry, analysis, and physics, as well as in cryptography.

Lattice Reduction: Finding Small Vectors in Practice

- Small vectors in a lattice may always be found by an exhaustive search. The exhaustive search algorithm is exponential in the dimension of the lattice.
- The most important modern advance in the algorithmic theory of lattice reduction (i.e., finding small vectors in lattices) is the LLL method of Lenstra, Lenstra and Lovász.

  A.K. Lenstra, H.W. Lenstra Jr., L. Lovász, Factoring polynomials with rational coefficients, *Mathematische Annalen* **261** (1982), 513–534.
- LLL finds a moderately small vector in polynomial time.
- LLL was invented *before* lattices became important in cryptography. Lattice reduction is of independent interest in many fields.
- Improvements to LLL are due to Schnorr, Euchner, and others (deep insertions, block reduction, pruning). But finding very short vectors remains exponentially difficult.
- LLL has numerous applications in signal processing, combinatorics, computer algebra, algebraic number theory, Diophantine equations and physics, as well as cryptography.
- There is widespread interest in LLL and lattice reduction:
  * The original LLL article was cited in 146 research articles (1986–1999).
  * The LLL algorithm is included in many computer packages, including:
    Mathematica, Maple, Pari, Simath, NTL,…
  * The LLL algorithm is featured in numerous books.

Lattice-Based Cryptosystems

Ajtai and Dwork (1997) and Goldreich, Goldwasser, and Halevi (1997) have recently proposed public key cryptosystems based on lattice problems. In both cases the public key consists of an entire basis for the lattice, so the key size is on the order of N^2 bits for a lattice of dimension N. For this reason, they require very large keys (around 1MB) to be secure, which makes them impractical.

Earlier knapsack cryptosystems (Merkle-Hellman, Chor-Rivest) were also broken using LLL because their underlying lattices, at practical key sizes, have relatively small dimension and other undesirable characteristics.

The NTRUEncrypt Public Key Cryptosystem is based on the closest and shortest vector problems (CVP and SVP). However, the NTRU lattice is associated to a quotient (convolution) ring and its public keys are associated to a cyclically generated basis for the lattice. An NTRUEncrypt public key has length on the order of N bits for a lattice of dimension N. (More accurately, approximately $(N/2)*\log_2(N/4)$ bits.)

This means that NTRU encryption can be practical, and indeed extremely fast. This is true even for lattices of dimension 500 to 1000, which are well beyond the reach of current technology to break.