



**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.

All the scrutiny to date has reaffirmed one simple fact: NTRUEncrypt, and the NTRU lattice, are secure. No attack has been found which significantly impacts the core ideas in NTRU technology. As with other public-key cryptosystems, it is of course possible to use these strong ideas in a weak way. Poor choices of parameters, or inappropriate message processing before encryption or after decryption, can reveal information to an attacker. However, the principles which underlie NTRU encryption, and which make it possible to have strong public-key cryptography at a fraction of the time and processing power previously necessary, remain unaffected by any research.

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, an 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. At that time he distributed a large number of preprints giving a full description of the algorithm and a preliminary security analysis. This preprint was also made available via the NTRU Cryptosystems website. Based on numerous comments from leading cryptographers, including Don Coppersmith, Johan Håstad, Andrew Odlyzko, and Adi Shamir, the security analysis was refined. 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 published in the proceedings of the Algorithmic Number Theory Symposium (ANTS III, Portland 1998). The NTRU algorithm has been subjected to a considerable amount of public scrutiny. Each of the relevant papers are discussed in detail below. These papers do **not** expose any security weaknesses in NTRU’s core technology. Instead, they show how inappropriate use of this technology can cause vulnerabilities, and re-validate the underlying security.

In order to describe more fully the extensive peer review of NTRU technology, we must first 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, it is often shorthand for “an analysis of an attack.” For example, the paper “A chosen-ciphertext attack against NTRU” (by Jaulmes and Joux) presents a chosen-ciphertext attack and then studies its effectiveness. The paper concludes with the observation that this attack is **not** effective against NTRUEncrypt when NTRUEncrypt is deployed with well-known techniques for defending against such attacks (cf. NTRU Technical Note #16, referenced in the bibliography below; these techniques are built into every implementation of NTRU security).
- 2) All cryptosystems are subject to certain classes of attacks. For example, chosen-ciphertext attacks exist for all public key cryptosystems, including RSA, ECC, and NTRUEncrypt. Such attacks do not affect the security of the underlying cryptographic algorithm, but instead they rely on sending specially constructed fake messages and observing the resulting decryptions. For each cryptosystem, there are straightforward techniques for defending against such attacks. The attacks are only effective if these simple precautions are not taken.

- 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.

NTRU security has an extremely distinguished history of peer review. 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 the defense is also completely analogous – one just uses parameter choices that make such attacks infeasible.

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. Nguyen and Stern, who have used lattice reduction techniques to crack several famous cryptosystems, studied NTRU technology and wrote, “It seems that better attacks or better lattice reduction algorithms are required in order to break NTRU.”

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. Moreover, as security parameters are increased, NTRU's advantages over both RSA and ECC increase as well. (In other words, at RSA 2048 levels of security, NTRU's speed advantage is even greater than it is at RSA 1024 levels of security!).

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 P. Garrett's book [Making, Breaking Codes: An Introduction to Cryptology](#) (Prentice-Hall, 2001).

It is precisely this high quality and volume of ongoing independent scrutiny that continuously and strongly reaffirms the security of NTRU technology.

2. Scrutiny of the NTRU Cryptosystem

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

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

Gentry presented a clever attack that would work against NTRUEncrypt if NTRUEncrypt were ever deployed with the security parameter N not a prime number. His research does not impact NTRUEncrypt's security in practice, because, from its introduction, NTRU 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 authors, two of the most respected names in the field of lattice-based techniques in cryptography, survey the use of lattices in both making and breaking cryptosystems. With regard to NTRUEncrypt (then known simply as NTRU), they conclude: "this makes NTRU the leading candidate among knapsack-based and lattice-based cryptosystems, and allows high dimension lattices," and "It seems that better attacks or better lattice reduction algorithms are required in order to break NTRU."

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

J. Hoffstein, J. H. Silverman, Protecting NTRU against chosen ciphertext and reaction attacks, NTRU Technical Report 016, 2000, see <http://www.ntru.com/technology/techpapers/tech.technical.abstracts.htm>.

Chosen-ciphertext attacks exist for all public key cryptosystems, including RSA, ECC and NTRUEncrypt. Such attacks do not affect the security of the underlying cryptographic algorithm, but instead they rely on sending specially constructed fake messages and watching to see what happens. The Jaulmes-Joux paper presents interesting new material in this direction and further highlights the need to use industry-standard enveloping techniques in order to protect against chosen-ciphertext and other reaction-type attacks. The encoding method of Fujisaki and Okamoto described in NTRU Technical Note #016, "Protecting NTRU Against Chosen Ciphertext and

Reaction Attacks”, provides a provably secure digital envelope for NTRUEncrypt that prevents attacks of this kind. Similar protections are available in the literature for RSA and ECC.

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, see <http://www.ntru.com/technology/techpapers/tech.technical.abstracts.htm>.

NTRU keys contain sequences 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].

This paper notes that the best way to attack NTRUEncrypt is via the techniques of lattice reduction and describes 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 the defense is also completely analogous – one just uses parameter choices that make such attacks infeasible.

These papers exemplify the quality of the ongoing independent scrutiny and analysis of NTRUEncrypt, which consistently reaffirms its security.

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.
- 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.
- 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 Wolfgang Goethe-Universität, 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

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

NTRU Cryptosystems Technical Notes

These are available from

<http://www.ntru.com/technology/techpapers/tech.technical.abstracts.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
- #017 Enhanced Encoding and Verification Methods for the NTRU Signature Scheme

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, *Combinatorica* 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. Micciancio, 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 Merkle-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.

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, the most effective known attacks on NTRU involve solving an SVP or a CVP. (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

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

where $\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_N$ 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 $2^N \text{Covolume}(L)$ 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 (2nd 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 $(N/2) \cdot \log_2(N/4)$ bits.)

Nguyen and Stern (CaLC-2001) note that, “this makes NTRU the leading candidate among knapsack-based and lattice-based cryptosystems, and allows high dimension lattices.”

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.