NTRU Bibliography

W. D. Banks, I. E. Shparlinski, A Variant of NTRU with Non-invertible Polynomials, INDOCRYPT 2002, Hyderabad, India, LNCS vol. 2551, Springer, 2002.

J. Buchmann, C. Ludwig, Practical Lattice Basis Sampling Reduction, ANTS 2006, 2006.

M. Coglianese, B.-M. Goi, MaTRU, A New NTRu-Based Cryptosystem, ACISP Progress in Cryptology - INDOCRYPT 2005: 6th International Conference on Cryptology in India 2005, Bangalore, India, Springer-Verlag, 2005.

D. Coppersmith, A. Shamir, Lattice attacks on NTRU http://www.springerlink.com/content/en3mrt3w8056lg25/?p=73f16332778348feb72e473abc182d81&pi=4, Advances in Cryptology - EUROCRYPT 1997, Konstanz, Germany, LNCS vol. 1233, Springer-Verlag, 1997.

B. Driessen, A. Poschmann, C. Paar, Comparison of innovative asymmetric signature schemes for WSNs, ACM WiSec 2008, Alexandria, VA, USA, 2008.

P. Gaborit, J. Ohler, P. Sole, CTRU, a polynomial analogue of NTRU, NTRU Technical Report #Inria RR-4621 , 2006.

N. Gama, N. Howgrave-Graham, H. Koy, P. Q. Nguyen, Rankin's Constant and Blockwise Lattice Reduction, Advances in Cryptology - CRYPTO 2006, Santa Babara, CA, LNCS vol. 4117, Springer-Verlag, 2006.

N. Gama, N. Howgrave-Graham, P. Nguyen, Symplectic Lattice Reduction and NTRU, Advances in Cryptology - EUROCRYPT 2006, 2006.

N. Gama, P. Nguyen, New Chosen-Ciphertext Attacks on NTRU, Public Key Cryptography - PKC 2007: 10th International Conference on Practice and Theory in Public-Key Cryptography 2007, Beijing, China, Springer-Verlag, 2007.

C. Gentry, Key Recovery and Message Attack on NTRU-Composite, Advances in Cryptology - EUROCRYPT 2001, Innsbruck, Austria, LNCS vol. 2045, Springer-Verlag, 2001.

C. Gentry, J. Jonsson, J. Stern, M. Szydlo, Cryptanalysis of the NTRU Signtare Scheme (NSS) from Eurocrypt 2001, Advances in Cryptology - ASIACRYPT 2001, 2001.

C. Gentry, M. Szydlo, Cryptanalysis of the revised NTRU Signature Scheme, Advances in Cryptology - EUROCRYPT 2002, 2002.

D. Han, J. Hon, J. W. Han, and D. Kwon, Key recovery attacks on NTRU without ciphertext validation routine, ACISP 2003, Wollongong, Australia, LNCS vol. 2727, Springer-Verlag, 2003.

S. Hasegawa, S. Isobe, M. Mambo, H. Shizuya, Y. Futa, M. Ohmori, A Countermeasure for Protecting NTRUSign against the Transcript Attack, 2007.

P. Hirschhorn, J. Hoffstein, N. Howgrave-Graham, W. Whyte, Choosing NTRU Parameters in Light of Combined Lattice Reduction and MITM approaches, ACNS 2009, 2009.

J. Hoffstein, N. Howgrave-Graham, J. Pipher, J. Silverman, W. Whyte, Performace Improvements and a Baseline Parameter Generation Algorithm for NTRUSign, WMPTC 2005, 2005.

J. Hong, J. W. Han, D. Kwon, D. Han, Imperfect Decryption and an Attack on the NTRU Encryption Scheme,

Cryptology ePrint Archive, ref. 2002/188, 2002.

N. Howgrave-Graham, J. H. Silverman, W. Whyte, A meet-in-the-middle attack on an NTRU private key, NTRU Technical Report #004, 2003.

N. Howgrave-Graham, J. Pipher, J. H. Silverman, W. Whyte, NAEP: Provable Security in the Presence of Decryption Failures, 2003.

N. Howgrave-Graham, P. Q. Nguyen, D. Pointcheval, J. Proos, J. Silverman, A. Singer, W. Whyte, The Impact of Decryption Failures on the Security of NTRU Encryption, Advances in Cryptology - CRYPTO 2003, Santa Babara, CA, LNCS vol. 0000, Springer-Verlag, 2003.

N. Howgrave-Graham, J. Pipher, J. H. Silverman, W. Whyte, Choosing Parameter Sets for NTRUEncrypt with NAEP and SVES-3, CT-RSA 2005, 2005.

N. Howgrave-Graham, J. Pipher, J. H. Silverman, W. Whyte, On Estimating the Lattice Security of NTRU, 2005.

N. Howgrave-Graham, Isodual Reduction of Lattices, Cryptology ePrint Archive, ref. 2007/105, 2007.

N. Howgrave-Graham, A Hybrid Lattice-Reduction and Meet-in-the-Middle Attack Against NTRU, Advances in Cryptology - CRYPTO 2007, Santa Babara, CA, LNCS vol. 4622, Springer-Verlag, 2007.

E. Jaulmes, A. Joux, A chosen-ciphertext attack against NTRU, Advances in Cryptology - CRYPTO 2000, Santa Babara, CA, LNCS vol. 0000, Springer-Verlag, 2000.

K. Kadati, K. Bhimavarapu, George Koodarappally, Capabilities and Performance of a JCE Implementation of NTRU Public Key Cryptosystem , Project Specification ECE 646 2005, George Mason University, 2005.

J.-P. Kaps, Cryptography for Ultra-Low Power Devices (PhD dissertation), 2006.

R. Kouzmenko, Generalizations of the NTRU Cryptosystem, 2006.

M. Lee, J. Kim, J. Song, K. Park, Sliding Window Method for NTRU, ACNS 2007, Zhuhai, China, LNCS vol. 4521, Springer, 2007.

R. Lindner, Current Attacks on NTRU, 2006.

R. Lindner, Analysis of Ntrusign, 2008.

R. Lindner, J. Buchmann, M. Doering, Efficiency Improvements for NTRU, Sicherheit 2008, LNI vol. 128, 2008.

X. Lv, B. Yang, C. Pei, Efficient Traitor Tracing Scheme Based On NTRU, PDCAT 2005, Dalian, China, 2005.

T. Meskanen, A. Renvall, A Wrap Error Attack Against NTRUEncrypt, WCC 2003, Versailles, France, 2003.

S. Min, G. Yamamoto, K.Kim, Weak property of malleability in NTRUSign, ACISP 2004, Sydney, Australia, LNCS vol. 3108, Springer-Verlag, 2004.

P. Mol, M. Yung, Recovering NTRU Secret Key from Inversion Oracles, PKC 2007, Barcelona, Spain, LNCS vol. 4939,

Springer, 2007.

M. Naslund, I. Spharlinski, W. Whyte, On the Bit Security of NTRUEncrypt, PKC 2003, Miami, FL, LNCS vol. 2567, Springer-Verlag, 2003.

P. Q. Nguyen, J. Stern, The Two Faces of Lattices in Cryptology, CaLC 2001, Providence, RI, LNCS vol. 2146, Springer-Verlag, 2001.

P. Q. Nguyen, D. Pointcheval, Analysis and Improvements of NTRU Encryption Paddings, Advances in Cryptology - CRYPTO 2002, Santa Babara, CA, LNCS vol. 0000, Springer-Verlag, 2002.

P. Q. Nguyen, O. Regev, Learning a Parallelepiped: Cryptanalysis of GGH and NTRU Signatures, Journal of Cryptology , .

P. Q. Nguyen, A Note on the Security of NTRUSign, Cryptology ePrint Archive, ref. 2006/387, 2006.

C. M. O'Rourke , Efficient NTRU Implementations (Master's Thesis), 2002.

J. Proos, Imperfect Decryption and an Attack on the NTRU Encryption Scheme, Cryptology ePrint Archive, ref. 2003/002, 2003.

T. E. Seidel, D. Socek, M. Sramka, Parallel Symmetric Attack on NTRU using Non-Deterministic Lattice Reduction, 2004.

J. H. Silverman, W. Whyte, Estimating Decryption Failure Probabilities for NTRUEncrypt, NTRU Technical Report #018, 2003.

J. H. Silverman, W. Whyte, Timing attacks on NTRUEncrypt via variation in the number of hash calls, CT-RSA 2007, 2007.

N. Smart, K. Geissler, Computing the $M = U U^t$ integer matrix decomposition, Cryptography and Coding 2003, Cirencester, UK, Springer, 2003.

N. Smart, F. Vercauteren, J. H. Silverman, An algebraic approach to NTRU (q = 2^n) via Witt vectors and overdetermined systems of nonlinear equations., SCN 2004, Amalfi, Italy, LNCS vol. 3352, Springer, 2004.

B. Sunar, C. M. O'Rourke, Achieving NTRU with Montgomery Multiplication, IEEE Transactions on Computers, Special Issue on Cryptographic Hardware and Embedded Systems, 52(4) 2003, 2003.

M. Szydlo, Hypercubic Lattice Reduction and Analysis of GGH and NTRU Signatures, Advances in Cryptology - EUROCRYPT 2003, 2003.

M. Szydlo, Hypercubic Lattice Reduction and Analysis of GGH and NTRU Signatures, Advances in Cryptology - EUROCRYPT 2003, 2003.

N. Vats, Algebraic Cryptanalysis of CTRU Cryptosystem, COCOON 2008, Dalian, China, Springer, 2008.

J. Yao, G. Zeng, Enhanced NTRU cryptosystem eliminating decryption failures,