Awesome Lattice-Based Cryptography

Kurt Pan

May 6, 2025

Contents

A curated list of awesome resources for learning and using lattice-based cryptography.

0.0.1 Surveys & Books

Title	Time	Authors/Team	URL
The LLL Algorithm: Survey and Applications	2009	Phong Q. Nguyen, Damien Stehlé	Link
A Decade of Lattice Cryptography	2016	Chris Peikert	Link
Fundamentals of Lattice Cryptography (Course Notes)	Ongoing	Daniele Micciancio, Oded Regev	Link
Lattice Basis Reduction: An Introduction to the LLL Algorithm and Its Applications	2002	Daniele Micciancio, Shafi Goldwasser	Micciancio and Goldwasser [2002a] (Book)
Complexity of Lattice Problems: A Cryptographic Perspective	2002	Daniele Micciancio, Shafi Goldwasser	Micciancio and Goldwasser [2002b] (Book)

0.0.2 Tutorials & Courses

Title	Time	Authors/Team	URL
Kyber and Dilithium	2024	Alfred Menezes	Link
The Mathematics of Lattice-Based Cryptography	2025	Alfred Menezes	Link
Lattice Cryptography Tutorial (Various Conferences)	Various	Chris Peikert	Example (Crypto 2011)
Introduction to Lattice-Based Cryptography (Bar-Ilan Winter School)	2015	Vadim Lyubashevsky	Link

0.0.3 Blogs & Talks

Title	Time	Authors/Team	URL
Prepping for post-quantum: a beginner's guide to lattice cryptography	2025	Cloudflare	Link
Chris Peikert's Blog (Lattice-Based Crypto Posts)	Various	Chris Peikert	Link (Check publications/talks section)
Vadim Lyubashevsky's Publications/Talks	Various	Vadim Lyubashevsky	Link
Windows on Theory (Blog posts on LWE, etc.)	Various	Various (e.g., Oded Regev)	Link
Real World Crypto Symposium Talks (Search for lattice topics)	Annual	Various Speakers	Link
Zama Blog (Focus on FHE)	Ongoing	Zama Team	Link

0.0.4 Key Papers

Foundational & Hardness Assumptions

Title	Time	Authors/Team	Citation
Generating hard instances of lattice problems	1996	Miklós Ajtai	Ajtai [1996]
On Lattices, Learning with Errors, Random Linear Codes, and Cryptography	2005	Oded Regev	Regev [2005]
The Learning with Errors Problem	2010	Oded Regev	Regev [2010]
On Ideal Lattices and Learning with Errors over Rings	2010	Vadim Lyubashevsky, Chris Peikert, Oded Regev	Lyubashevsky et al. [2010]

Public-Key Encryption (PKE) & Key Encapsulation Mechanisms (KEM)

Title	Time	Authors/Team	Citation
NTRU: A Ring-Based Public Key Cryptosystem	1998	Jeffrey Hoffstein, Jill Pipher, Joseph H. Silverman	Hoffstein et al. [1998]
Post-quantum key exchange - a new hope	2015	Erdem Alkim, Léo Ducas, Thomas Pöppelmann, Peter Schwabe	Alkim et al. [2015]
CRYSTALS-Kyber: Algorithm Specifications and Supporting Documentation	2017+	Kyber Team	Kyber Team

Digital Signatures

Title	Time	Authors/Team	Citation
Trapdoors for Hard Lattices and New Cryptographic Constructions	2008	Craig Gentry, Chris Peikert, Vinod Vaikuntanathan	Gentry et al. [2008]
Falcon: Fast-Fourier Lattice-based Compact Signatures over NTRU	2017+	Falcon Team	Falcon Team
CRYSTALS-Dilithium: Algorithm Specifications and Supporting Documentation	2017+	Dilithium Team	Dilithium Team

Fully Homomorphic Encryption (FHE)

Title	Time	Authors/Team	Citation
Fully homomorphic encryption using ideal lattices	2009	Craig Gentry	Gentry [2009]
Fully Homomorphic Encryption without Bootstrapping	2011	Zvika Brakerski, Vinod Vaikuntanathan	Brakerski and Vaikuntanathan [2011]
(Leveled) fully homomorphic encryption without modulus switching	2012	Zvika Brakerski	Brakerski [2012]
Homomorphic Encryption from Learning with Errors: Conceptually-Simpler, Asymptotically-Faster, Attribute-Based	2013	Craig Gentry, Amit Sahai, Brent Waters	Gentry et al. [2013]
TFHE: Fast Fully Homomorphic Encryption over the Torus	2016	Ilaria Chillotti, Nicolas Gama, Mariya Georgieva, Malika Izabachène	Chillotti et al. [2016]

0.0.5 Software Libraries

Title	Language	Authors/Team	Description	URL
PALISADE Homomorphic Encryption Library	C++	PALISADE Team (NJIT, Duality Technologies, et al.)	Homomorphic Encryption Library	Link
Microsoft SEAL (Simple Encrypted Arithmetic Library)	C++	Microsoft Research	Simple Encrypted Arithmetic Library	Link
HElib (Homomorphic Encryption Library)	C++	IBM Research	Homomorphic Encryption Library	Link
NFLlib (Number Field Lattice Library)	C++	Various Contributors	Number Field Lattice Library	Link
Open Quantum Safe (liboqs)	C	OQS Project	Includes implementations of NIST PQC candidates	Link
FHEW / TFHE	C++/C	Various Contributors	Fast FHE libraries based on GSW/torus	Link
Lattigo	Go	Tune Insight	Go library for lattice crypto, including HE	Link

0.0.6 Standardization Efforts

Title	Time	Authors/Team	URL
NIST Post-Quantum Cryptography (PQC) Standardization	2016-Present	NIST & Community	Link
HomomorphicEncryption.org Standards	Ongoing	Community	Link

Contributions welcome! Please open an issue or pull request to suggest additions or corrections.

Bibliography

M. Ajtai. Generating hard instances of lattice problems. In *STOC '96: Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, pages 99–108. ACM, 1996. doi: 10.1145/237814.237838. URL `https://dl.acm.org/doi/10.1145/237814.237838`.

E. Alkim, L. Ducas, T. P\\"oppelmann, and P. Schwabe. Post-quantum key exchange - a new hope, 2015. URL `https://eprint.iacr.org/2015/1092`.

Z. Brakerski. (Leveled) fully homomorphic encryption without modulus switching, 2012. URL `https://eprint.iacr.org/2011/344`.

Z. Brakerski and V. Vaikuntanathan. Fully Homomorphic Encryption without Bootstrapping, 2011. URL `https://eprint.iacr.org/2011/277`.

I. Chillotti, N. Gama, M. Georgieva, and M. Izabach\\`ene. Tfhe: Fast Fully Homomorphic Encryption over the Torus, 2016. URL `https://eprint.iacr.org/2016/421`.

Dilithium Team. Crystals-Dilithium: Algorithm Specifications and Supporting Documentation.

Falcon Team. Falcon: Fast-Fourier Lattice-based Compact Signatures over NTRU.

C. Gentry. Fully homomorphic encryption using ideal lattices. In *STOC '09: Proceedings of the 41st annual ACM symposium on Theory of computing*, pages 169–178. ACM, 2009. doi: 10.1145/1536414.1536440. URL `https://dl.acm.org/doi/10.1145/1536414.1536440`.

C. Gentry, C. Peikert, and V. Vaikuntanathan. Trapdoors for Hard Lattices and New Cryptographic Constructions. In *STOC '08: Proceedings of the 40th annual ACM symposium on Theory of computing*, pages 197–206. ACM, 2008. doi: 10.1145/1374376.1374407. URL `https://dl.acm.org/doi/10.1145/1374376.1374407`.

C. Gentry, A. Sahai, and B. Waters. Homomorphic Encryption from Learning with Errors: Conceptually-Simpler, Asymptotically-Faster, Attribute-Based, 2013. URL `https://eprint.iacr.org/2013/340`.

J. Hoffstein, J. Pipher, and J. H. Silverman. Ntru: A Ring-Based Public Key Cryptosystem. In J. P. Buhler, editor, *Algorithmic Number Theory, ANTS-III*, volume 1423 of *Lecture Notes in Computer Science*, pages 267–288. Springer, 1998. doi: 10.1007/BFb0054868. URL `https://link.springer.com/chapter/10.1007/BFb0054868`.

Kyber Team. Crystals-Kyber: Algorithm Specifications and Supporting Documentation.

V. Lyubashevsky, C. Peikert, and O. Regev. On Ideal Lattices and Learning with Errors over Rings. In H. Gilbert, editor, *Advances in Cryptology – EUROCRYPT 2010*, volume 6110 of *Lecture Notes in Computer Science*, pages 1–23. Springer, 2010. doi: 10.1007/978-3-642-13190-5_1. URL `https://link.springer.com/chapter/10.1007/978-3-642-13190-5_1`.

D. Micciancio and S. Goldwasser. *Lattice Basis Reduction: An Introduction to the LLL Algorithm and Its Applications.* The Springer International Series in Engineering and Computer Science. Springer, 2002a. ISBN 978-1-4615-0715-9. doi: 10.1007/978-1-4615-0715-9. URL `https://doi.org/10.1007/978-1-4615-0715-9`.

D. Micciancio and S. Goldwasser. *Complexity of Lattice Problems: A Cryptographic Perspective.* The Springer International Series in Engineering and Computer Science. Springer, 2002b. ISBN 978-1-4615-0897-7. doi: 10.1007/978-1-4615-0897-7. URL `https://doi.org/10.1007/978-1-4615-0897-7`.

O. Regev. On Lattices, Learning with Errors, Random Linear Codes, and Cryptography. In *STOC '05: Proceedings of the thirty-seventh annual ACM symposium on Theory of computing*, pages 84–93. ACM, 2005. doi: 10.1145/1060590.1060603. URL `https://dl.acm.org/doi/10.1145/1060590.1060603`.

O. Regev. The Learning with Errors Problem, 2010. Invited survey in CCC 2010.