Léo Ducas

Born in Toulon, France, on Oct. 19, 1986

Eerste Atjehstraat 140E, 1094 KV Amsterdam, The Netherlands.

+31 6 20 80 58 32 | ducas@cwi.nl | homepages.cwi.nl/~ducas/ | lducas

"My work is a game, a very serious game" M.C. Escher

Research Interest

Research area: Lattice-based cryptography.

- **Quantum and concrete cryptanalysis,** New algorithms, Tweaks for practice, Security estimates
- **Optimizing cryptographic designs,** New algorithms, Transfer from theory to practice, Standardization
- **Open-Source Implementation,** Code and Data Sharing, Strengthening Knowledge, Accelerating discoveries

Employent

Centrum Wiskunde & Informatica (CWI) *Amsterdam, The Netherlands*

Research Staff in the Cryptology department *2015-Present*

University of California, San-Diego (UCSD) *San Diego, C.A., United-States*

Postdoc in the Computer Science and Engineering department *2013-2014*

Supervised by Pr. Daniele Micciancio

Education

École Normal Supérieure (ENS) *Paris, France*

Ph.D., Lattice Based Signatures: Attacks, Analysis and Optimizations *2009-2013*

Advisors: Pr. Phong Q. Nguyen And Pr. David Pointcheval

Master MPRI (Parisian Master of Research in Computer Science). With honours. *2007-2009*

Main topics: Formal Languages and Automated Proofs, Complexity, Game Theory, Cryptography
Thesis: Conception of a Language for Cryptographic Reduction. Supervised by Mathieu Baudet.

Double Bachelor Degree: Mathematics and Computer Science. with honours. *2006-2007*

Awards

2017 **Honorable mention,** Eurocrypt, for *Short Stickelberger Class relations and application to Ideal-SVP*

2016 **Internet Defense Prize,** USENIX & Facebook, for *Post-Qunatum Key Exchange – A New Hope* *100 000 $ / 4*

2015 **NTRU challenge,** Cryptanalysis of NTRU challenges *5 x 1 000 $ / 2*

Grants

Veni Personal Research Grant from NWO *250 000 €*

Project: Cryptanalysis of Lattice-based Cryptography *2017-2020*

Public-Private Partnership Grant (CWI & NXP-Semiconductors) *160 000 €*

Post-Quantum Cryptography *2016-2017*

Popular Science Project, from INRIA and Cap'Math *20 000 €*

Cryptris, a video game about public key cryptography *2012-2014*

Scientific Activities

Workshop: Mathematical Structures for Cryptography *Lorrentz Center, Leiden, The Netherlands*

Co-organized with Hendrik Lenstra, Alice Silverberg, Marco Streng. *22-26 Aug. 2016*

Workshop: FPLLL Days — *CWI, Amsterdam, The Netherlands*

Co-organized with Marc Stevens, Martin Albrecht. — *06-14 Jul. 2017*

Program Committee Member

PKC 2016, AfricaCrypt 2016, PKC 2017, STACS 2017, EuroCrypt 2017, PKC 2018

Teaching

Courses

Lattice Algorithms and Applications to Cryptology — *MasterMath, The Netherlands*

16 lectures of 2h45, Co-lectured with Daniel Dadush. — *Spring 2018*

Tutorials

Mar. 2017 **Course: Lattice-based Crypto: Construction and Cryptanalysis,** Spring School on Lattice-Based Cryptography (6 hours, with Exercises) — *U. of Oxford, UK*

Jun. 2016 **Course: Introduction to Lattice Based Cryptography,** African Mathematical School on Cryptography (8 hours: Lecture notes) — *U. of Bamenda, Cameroon*

Oct. 2015 **Two lectures: LLL and BKZ, Recovering short generators…,** Mathematical and Practical Aspects of Fully Homomorphic Encryption and Multi-Linear Maps — *Institut Henry Pointcaré, France*

Jun. 2015 **One Lecture: SIS-based constructions,** Summer school on real-world crypto and privacy — *Šibenik, Croatia*

Supervision

2016 – **Ph.D.,** Koen de Boer

2017 **Ph.D. Internship (3 Months),** Guillaume Bonnoron (from U. of Rennes, France)

2016 **Internship (6 Months),** Willy Quash (from ENS Lyon, France)

Master Thesis, Alex van Poppelen (from Utrecht U., The Netherlands)

Bachelor Thesis, Wessel P.J. van Woerden (from Leiden U., The Netherlands)

Ph.D. Internship (3 Months), Yang Yu (from Tsinghua U., China)

Skills

Programming Languages C/C++, Python, SageMath, LaTeX, git, Ocaml

French (native), English (fluent), Dutch (beginner)

Presentations (Since 2015)

Conferences

Jul. 2016 **Fast Fourier Orthogonalization,** ISSAC 2016 — *Wilfrid Laurier U., Waterloo, Canada*

May 2016 **Recovering Short Generators of Principal Ideals in Cyclotomic Rings,** Eurocrypt 2016 — *Vienna, Austria*

Nov. 2015 **Recovering Short Generators of Principal Ideals in Cyclotomic Rings,** Elliptic Curve Cryptography — *U. of Bordeaux, France*

Apr. 2015 **FHEW: Bootstrapping in Less than a Second,** Eurocrypt 2015 — *Sofia, Bulgaria*

Workshops

Apr. 2017 **Short Stickelberger Class Relations and application to Ideal-SVP,** Frontiers of Quantum Safe Cryptography — *U. Paris VI, France*

Jan. 2017 **Exploiting Quantum Algorithms against Ideal-SVP,** Perspectives on Complexity Theory and Cryptography — *IISc, Bengalore, India*

Nov. 2016 **Post-Quantum Cryptography from Lattices,** QuSoft Symposium — *CWI, Amsterdam, The Netherlands*

Nov. 2016 **NewHope, Frodo, in Between and Beyond,** European Cyber Week — *U. of Rennes, France*

Nov. 2016 **Introduction to homomorphic encryption,** Colloquium Coding Theory and Cryptography — *Royal Flemish Academy, Brussel, Belgium*

Nov. 2016 **NewHope, Frodo, in Between and Beyond,** Quantum-Safe Crypto Workshop — *National University of Singapore*

Oct. 2016 **Short stickelberger class relations and application to ideal-SVP,** Mathematics of Information-Theoretic Cryptography — *Institute for Mathematical Sciences, Singapore*

Jul. 2016 **A subfield lattice attack on overstretched NTRU assumptions,** Homomorphic Encryption Applications and Technology — *Institute Henry Pointcaré, France*

May 2016 **What you should know on Lattice-based Cryptography to implement it,** Cryptographic protocols for small devices — *Vienna University of Technology, Austria*

Oct. 2015 **Recovering Short Generators of Principal Ideals in Cyclotomic Rings**, Tools for Asymmetric Cryptanalysis — *Bochum, Germany*

Nov. 2015 **Recovering Short Generators of Principal Ideals in Cyclotomic Rings**, Conference on Mathematics of Cryptography — *Sloan Foundation, UC Irvine, USA*

Apr. 2015 **Recovering Short Generators of Principal Ideals in Cyclotomic Rings**, Mathematics of Lattices and Cybersecurity — *ICERM, Providence, USA*

Seminars

Mar. 2017 **Short Stickelberger Class Relations and application to Ideal-SVP**, Monthly Lattice Meeting — *ENS Lyon, France*

Dec. 2016 **Post-Quantum Cryptography from Lattices**, CWI Scientific Meeting — *CWI, Amsterdam, The Netherlands*

Apr. 2016 **What you should know on Lattice-based Cryptography to implement it**, Cryptography Seminar — *Royal Holloway, UK*

Apr. 2016 **New directions in nearest neighbor searching with applications to lattice sieving**, COMMSP Seminar — *Imperial College, UK*

Dec. 2015 **Fast Fourier Orthogonalization**, Séminaire CCA — *Télécom-ParisTech, France*

Nov. 2015 **New directions in nearest neighbor searching with applications to lattice sieving**, Monthly Lattice Meeting — *ENS Lyon, France*

Jun. 2015 **Recovering Short Generators of Principal Ideals in Cyclotomic Rings**, Seminaire Polsys — *U. Paris VI, France*

May 2015 **Recovering Short Generators of Principal Ideals in Cyclotomic Rings**, Cryptography Working Group — *Utrecht, The Netherlands*

Apr. 2015 **Recovering Short Generators of Principal Ideals in Cyclotomic Rings**, LACAL Seminar — *EPFL, Switzerland*

Feb. 2015 **Exploration of the log-unit lattice** $\mathrm{Log}\,\mathbb{Z}[\zeta_2^n]^\times$, Monthly Lattice Meeting — *ENS Lyon, France*

Media

Coverage

Sep. 2016 **Https: nu ook bestand tegen de quantumcomputer**, Arnout Jaspers — *NEMO, Kennislink*

Jul. 2016 **Experimenting with Post-Quantum Cryptography**, Matt Braithwaite — *Google's Security blog*

Nov. 2015 **The Tricky Encryption That Could Stump Quantum Computers**, Peter Diamond — *Wired (reprint)*

Nov. 2015 **A Tricky Path to Quantum-Safe Encryption**, Peter Diamond — *Quanta Magazine*

Self-authored

Aug. 2015 **L'eldorado post-quantique**, Léo Ducas — *La Recherche*

Jan. 2015 **Un cryptographie Nouvelle: le réseau euclidien**, Léo Ducas — *Linux Magazine FR*

Dec. 2014 **Démocratiser la cryptographie**, Léo Ducas — *Linux Magazine FR*

Jun. 2015 **Les dessous géométriques de Cryptris**, Léo Ducas — *Images des Mathématiques (CNRS's blog)*

Jun. 2015 **Comprendre une des techniques les plus sophistiquées de cryptographie en... jouant à Tetris**, Anthony Teston, Mathieu Jouhet, Léo Ducas, Thierry Viéville — *Images des Mathématiques (CNRS's blog)*

Scientific Publications

Bibliometry

Peer-reviewed publications: 17 **H-index: 15** **Citations: 884**, according to Google Scholar

Pre-Prints and Reports

2017 **Advances on Quantum Cryptanalysis of Ideal Lattices**, Léo Ducas — *to appear in Nieuw Archief in Wiskunde*

CRYSTALS - Kyber: a CCA-secure module-lattice-based KEM, Joppe Bos, Léo Ducas, Eike Kiltz, Tancrède Lepoint, Vadim Lyubashevsky, John Schanck, Peter Schwabe, Damien Stehlé — *Submitted*

CRYSTALS – Dilithium: digital signatures from module lattices, Léo Ducas, Tancrède Lepoint, Vadim Lyubashevsky, Peter Schwabe, Gregor Seiler, Damien Stehlé — *Submitted*

Hash Proof Systems over Lattices Revisited, Fabrice Benhamouda, Olivier Blazy, Léo Ducas, Willy Quash — *Submitted*

On the Statistical Leak of the GGH13 Multilinear Map and some Variants, Léo Ducas, Alice Pellet–Mary — *Submitted*

Second Order Statistical Behavior of LLL and BKZ, Léo Ducas, Yang Yu — *Submitted*

2015 **Accelerating Bliss: the geometry of ternary polynomials**, Léo Ducas — *Tech. Report*

2013 **Lattice Based Signatures: Attacks, Analysis and Optimization**, Léo Ducas — *Ph.D. Thesis*

Peer-Reviewed Publications

2017	**The closest vector problem in tensored root lattices of type A and in their duals,** Léo Ducas, Wessel van Woerden	*Design, Codes and Cryptography*
	Short Stickelberger Class Relations and application to Ideal-SVP, Ronald Cramer, Léo Ducas, Benjamin Wesolowski	*EUROCRYPT '17*
2016	**Frodo: Take off the ring! Practical, Quantum-Secure Key Exchange from LWE,** Joppe Bos, Craig Costello, Léo Ducas, Ilya Mironov, Michael Naehrig, Valeria Nikolaenko, Ananth Raghunathan and Douglas Stebila	*CCS '16*
	A subfield lattice attack on overstretched NTRU assumptions, Martin Albrecht, Shi Bai and Léo Ducas	*CRYPTO '16*
	Fast Fourier Orthogonalization, Léo Ducas and Thomas Prest	*ISSAC '16*
	Post-Quantum Key Exchange – A New Hope, Erdem Alkim, Léo Ducas, Thomas Poeppelmann and Peter Schwabe	*USENIX security '16*
	Sanitization of FHE Ciphertexts, Léo Ducas and Damien Stehlé	*EUROCRYPT '16*
	New directions in nearest neighbor searching with applications to lattice sieving, Anja Becker, Léo Ducas, Nicolas Gama and Thijs Laarhoven	*SODA '16*
	Recovering Short Generators of Principal Ideals in Cyclotomic Rings, Ronald Cramer, Léo Ducas, Peikert and Oded Regev	*EUROCRYPT '16*
	FHEW: Bootstrapping Homomorphic Encryption in less than a second, Léo Ducas and Daniele Micciancio	*EUROCRYPT '15*
2014	**Efficient Identity-Based Encryption over NTRU Lattices,** Léo Ducas and Vadim Lyubashevsky and Thomas Prest	*ASIACRYPT '14*
	Improved Short Lattice Signatures in the Standard, Léo Ducas and Daniele Micciancio	*CRYPTO '14*
	Enhanced Lattice-Based Signatures on Reconfigurable Hardware, Thomas Pöppelmann and Léo Ducas and Tim Güneysu	*CHES '14*
2013	**Lattice Signatures and Bimodal Gaussians,** Léo Ducas and Alain Durmus and Tancrède Lepoint and Vadim Lyubashevsky	*CRYPTO '13*
2012	**Learning a Zonotope and More: Cryptanalysis of NTRUSign Countermeasures,** Léo Ducas and Phong Nguyen	*ASIACRYPT '12*
	Faster Gaussian Lattice Sampling using Lazy Floating-Point Arithmetic, Léo Ducas and Phong Nguyen	*ASIACRYPT '12*
	Ring-LWE in Polynomial Rings, Léo Ducas and Alain Durmus	*PKC '12*
2010	**Anonymity from Asymmetry: New Constructions for Anonymous HIBE,** Léo Ducas	*CT-RSA '10*