Léo Ducas

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

Sloterkade 42-II, 1058 HG 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: *Cryptology* (theory, practice, standards, cryptanalysis),
with a particular focus on *lattice-based* cryptographic systems.

- **Number theory and geometry of numbers,** For applications in 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

Employment

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

Research-Staff (tenured) in the Cryptology Group *2015-Present*

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

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

Hosted by Prof. Daniele Micciancio

Education

École Normale Supérieure (ENS) *Paris, France*

Ph.D. “Lattice Based Signatures: Attacks, Analysis and Optimization” *2009-2013*

Advisors: Prof. Phong Q. Nguyen And Prof. 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
Master Thesis: “Conception of a Language for Cryptographic Reduction”. Supervised by Mathieu Baudet.

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

Honors and Awards

2020-2025	**ERC Starting-Grant,** Project: A Reduction Theory For Codes and Lattices in Cryptography (ARTICULATE)	*1 500 000 €*
2020	**Research Fellow of the Simons Institute,** Research Semester on Lattices	*Berkeley, CA, USA*
2018–	**Co-leader of the Darmstadt SVP challenge Hall of Fame** ↗**,** Record computation for lattice problems	
2018	**Top 3 paper[2] at Asiacrypt,** for *Learning strikes again: the case of the DRS signature scheme*	
2017	**Top 3 paper[2] at Eurocrypt,** for *Short Stickelberger Class relations and application to Ideal-SVP*	
2017-2020	**Veni Personal Research Grant from NWO,** Project: Cryptanalysis of Lattice-based Cryptography	*250 000 €*
2016	**Facebook Internet Defense Prize** ↗ **at USENIX,** for *Post-Quantum Key Exchange – A New Hope*	*100 000 $ / 4*
2015	**NTRU challenge from Security Innonvation** ↗**,** Cryptanalysis of NTRU challenges	*5 x 1 000 $ / 2*

Program Committees and Editorial Boards

Editorial Boards

[2] A.k.a. “honorable mention”, paired with an invitation to submit to the Journal of Cryptology.

Journal *Mathematical Cryptology* ↗ *2020 –*

Program Committee Member

Conferences *PKC'16, AfricaCrypt'16, PKC'17, STACS'17, EuroCrypt'17, PKC'18, SCN'18, CRYPTO'18, Asiacrypt'18, PKC'19, LatinCrypt'19, EuroCrypt'20, EuroCrypt'21*

Trimester on Post-Quantum Algebraic Cryptography (Fall 2021) *Institut Henry Pointcaré, Paris*

Consortium Grants and Industrial Funding Acquisition

European H2020 Project (12 Institutions) *5 000 000 €/ 12*
PROMETHEUS: Advanced Lattice-Based Cryptography from Theory to Practice *2018-2022*
PI for CWI, and Work-Package Leader

Public-Private Partnership Grant (CWI & NXP-Semiconductors) *160 000 €*
Post-Quantum Cryptography *2016-2017*
Co-PI with Ronald Cramer

Teaching

Post-Doc Hosting

2019 **Benjamin Wesolowski**, Graduate from EPFL *Co-hosted with Ronald Cramer*
2018-2019 **Yang Yu**, Gratuate from Tsinghua University

PhD. Supervision

2018 – **Wessel P.J. van Woerden**, on Lattice Algorithms and Cryptanalysis
2016 – **Koen de Boer**, on Algebraic Number Theory and Quantum Algorithms

Bachelor and Master Thesis Supervision

2018 **Wessel P.J. van Woerden**, Master Thesis at Leiden U.
2016 **Wessel P.J. van Woerden**, Bachelor Thesis at Leiden U.
2017 **Alex van Poppelen**, Master Thesis at from Utrecht U.

Visiting Students

2020 **Oleksandra (Sasha) Lapiha**, Master Internship, visiting from ENS Paris
2019 **Alice Pellet–Mary**, Ph.D. Internship, Visiting from ENS Lyon *Funded by the CWI internship program*
2018 **Maxime Plançon**, Master Internship, visiting from ENS Paris
2017 **Guillaume Bonnoron**, Ph.D. Internship (3 Months), visiting from U. of Rennes *Funded by the CWI internship program*
2016 **Willy Quash**, Master Internship (6 Months), visiting from ENS Lyon
Yang Yu, Ph.D. Internship, Yang Yu visiting from from Tsinghua U., China) *Funded by the ERCIM program*

Courses

Lattice Algorithms and Applications to Cryptology *MasterMath, The Netherlands*
16 lectures of 2h45, Co-lectured with Daniel Dadush. With lecture notes ↗ *Spring 2018*

Tutorials

Mar. 2019 **Mini-Course: Algorithms for lattice problems**, Winter school on mathematical foundations of asymmetric cryptography (3 hours) *French Mathematical Society*
June 2018 **Lecture: Introduction to Fully Homomorphic Encryption**, Cyber in Occitanie (2 hours, plus Exercises ↗) *Montpelier, France, LIRMM and CNFM*
Mar. 2017 **Mini-Course: Lattice-based Crypto: Construction and Cryptanalysis**, Spring School on Lattice-Based Cryptography (6 hours, with Exercises ↗)) *U. of Oxford, UK*
Jun. 2016 **Mini-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 **Lecture: SIS-based constructions**, Summer school on real-world crypto and privacy *Šibenik, Croatia*

Invitations (Selection)

2020	**In Residence Fellow**, Research Semester on Lattices at the Simons Institute	*Berkeley, CA, USA*
May 2018	**Invited Speaker**, Workshop on Lattice Crypto and Algorithms, LATCA@BiCi (Z. Brakerski, V. Vaikuntanathan, H. Wee)	*Bertinoro, Italy*
May 2018	**Keynote speaker**, Africacrypt 2018	*Marrakesh, Morocco*
Apr. 2018	**Invited speaker**, Computational Challenges in the Theory of Lattices	*ICERM, Brown, USA*
Feb. 2018	**Research visit**, (Steven Galbraith)	*Aukland U., New-Zealand*
Twice	**Invited speaker**, HEAT Workshops (N. Smart, F. Verkauteren)	*Institute Henry Pointcaré, France*
Nov. 2015	**Invited Speaker**, Elliptic Curve Cryptography	*U. of Bordeaux, France*
Nov. 2015	**Invited Speaker**, Conference on Mathematics of Cryptography, Sloan Foundation (H. Lenstra and A. Silverberg)	*UC Irvine, USA*
Apr. 2015	**Invited Speaker**, Mathematics of Lattices and Cybersecurity, ICERM (J. Hoffstein)	*ICERM, Brown, USA*

Presentations

Conferences

May. 2018	**The General Sieve Kernel**, Africacrypt	*Marrakesh, Morocco*
May. 2018	**Large FHE gates from Tensored Homomorphic Accumulator**, Africacrypt	*Marrakesh, Morocco*
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

May 2020	**LWE with Side Information: Attacks and Concrete Security Estimation**, Lattices: From Theory to Practice	*Berkeley, CA, USA (online)*
Feb. 2020	**Self-Reducibility of Ideal-SVP via Arakelov Random Walks**, Lattices: Geometry, Algorithms and Hardness	*Berkeley, CA, USA*
Jan. 2020	**Algorithms for Algebraic Lattices: Classical and Quantum**, Lattices: Algorithms, Complexity, and Cryptography Boot Camp	*Berkeley, CA, USA*
May 2019	**Poly-Time BDD near Minkowski's Bound in Discrete Logarithm Lattices**, 5th London Symposium on Information Theory	*UK, King's College, London*
May. 2018	**The General Sieve Kernel**, Lattice Crypto and Algorithms	*LATCA@BiCi, Bertinoro, Italy*
Apr. 2018	**Logarithmic Lattices**, Computational Challenges in the Theory of Lattices	*ICERM, Brown, USA*
Sept. 2017	**Pruning in FPLLL, and Prototyping Lattice Algorithm with FPYLLL**, FPLLL days	*CWI, Amsterdam*
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

Aug. 2020	**An Algorithmic Reduction Theory for Binary Codes**, Tutte Colloquium	*U. of Waterloo, Canada (online)*
June 2020	**An Algorithmic Reduction Theory for Binary Codes**, CANTA Inaugural Seminar	*Royal Holloway, London (online)*
Nov. 2018	**The General Sieve Kernel**, Londonish Lattice Coding and Crypto Meeting	*TU/e, Utrecht*
Oct. 2018	**The General Sieve Kernel**, Séminaire Théorie des Nombres	*U. of Bordeaux, France*
Sep. 2018	**The General Sieve Kernel**, Londonish Lattice Coding and Crypto Meeting	*RHUL and Imperial College, London*
Sep. 2017	**Shortest Vector from Lattice Sieving: A Few Dimension for Free**, Monthly Lattice Meeting	*ENS Lyon, France*
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** $\operatorname{Log}\mathbb{Z}[\zeta_2^n]^\times$, Monthly Lattice Meeting	*ENS Lyon, France*

Technological Transfer

Candidates to the NIST Post-Quantum Cryptography Standardization Project

Co-author of *NewHope* **(industrial partners: ARM, NXP)**	*Post-Quantum Key Exchange* *Experimented in the wild by Google*
Co-author of *Frodo* **(industrial partners: NXP, Google, Microsoft)**	*Post-Quantum Key Exchange*
Co-author of *Kyber* **(industrial partners: IBM, NXP, SRI Int.)**	*Post-Quantum Key Exchange*
Co-author of *Dilithium* **(industrial partners: IBM, NXP, SRI Int.)**	*Post-Quantum Signature*

Initial Submission of these four candidates to the 1^{st} Round in December 2017	out of 72
All these four candidates have been selected for the 2^{nd} Round in January 2019	out of 28
Two candidates (Kyber and Dilithium) have been selected for the Final Round in July 2020	out of 7

Final Selection of a Portfolio of Standards Expected for the second half of 2021.

Others

Co-author and developer of *BLISS*	*Compact Lattice-Based Signatures*
Co-author and developer of *FHEW*	*Fully Homomorphic Encryption*

Services

Workshop and Seminar organization

Workshop: Mathematical Structures for Cryptography — *Lorentz 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*

Prometheus Consortium Meeting — *CWI, Amsterdam, The Netherlands*
Apr. 2019

RISC seminars — *CWI, Amsterdam, The Netherlands*
Co-organized with Ronald Cramer, Marc Stevens, and Serge Fehr — *2016 –*

Joint Online Seminar (CWI, Royal Holloway, ENS Lyon) — *Online*
Co-organized with Damien Stehle & Martin Albrecht — *2020 –*

Ph.D Examination

2018	**Guillaume Bonnoron**, Jury Member	*U. of Rennes*
2018	**Vincent Zucca**, Jury Member	*Sorbonne U., Paris*
2019	**Thomas Debris**, Jury Member and Thesis Dissertation Referee	*Sorbonne U., Paris*
2020	**Jiabo Wang**, Jury Member and Thesis Dissertation Referee	*Imperial College, London*

Others

2019-2020	**Open-Source and Open-Data Valorization Program**, Co-proposed to the IACR Board with Martin Albrecht	
2020	**Panel co-moderator**, Panel Discussion on Contact Tracing	*Eurocrypt 2020, Online*
2018–	**H2020 Consortium Administration and Coordination**, Work Package Leader and Board Member	*PROMETHEUS*

Media & Outreach

Coverage

Oct. 2019	**Post-quantum geheimschrift**, Dorine Schenk	*NRC*
Fev. 2019	**Le NIST a annoncé les protocoles qui seront...**, Philippe Pajot	*La Recherche*
May 2018	**Op zoek naar quantumbestendige cryptografie**, Pieter Edelman	*Bits and Chips*
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**, Natalie Wolchover	*Wired (reprint)*
Nov. 2015	**A Tricky Path to Quantum-Safe Encryption**, Natalie Wolchover	*Quanta Magazine*

Outreach

Nov. 2018	**Traquer les failles des Algorithmes**, Léo Ducas	*La Recherche*
Feb. 2018	**Preparing ourselves for the threats of the Post-Quantum Era**, Thijs Veugen, Thomas Attema, Maram van Heesch, Léo Ducas	*ERCIM NEWS*
Sept. 2017	**Advances on Quantum Cryptanalysis of Ideal Lattices**, Léo Ducas	*Nieuw Archief voor Wiskunde*
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. 2014	**Les dessous géométriques de Cryptris**, Léo Ducas	*Images des Mathématiques (CNRS's blog)*
Jun. 2014	**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)*

Collaborations

In the Netherlands

NL	**CWI, Cryptology Group**, Ronald Cramer, Marc Stevens	*Research, Software, H2020 Grant*
NL	**CWI, Algorithms and Complexity Group, QuSoft**, Stacey Jeffery, Ronald de Wolf	*Research*
NL	**CWI, Networks and Optimization Group**, Daniel Dadush	*Research*
NL	**Leiden U., Mathematical Institute**, Peter Bruin, Marco Streng, Hendrik Lenstra	*Teaching, Student (Co-)Supervision, Conf. Organization*
NL	**Radboud University Nijmegen, Digital Security Group**, Peter Schwabe	*Research, Software, Standardization*

International

FR	**ENS Lyon, Computing and Parallelism Lab., AriC Team**, Damien Stehlé	*Research, Student Supervision, Software*
SW	**IBM Zurich, Security Group**, Vadim Lyubashevsky, Thijs Laarhoven	*Research, Standardization, H2020 Grant*
BE	**NXP, Leuven, Innovation Center Crypto and Security**, Joppe Bos	*Research, Standardization, H2020 Grant*
USA	**New-York U., Courant Institute of Mathematical Sciences**, Oded Regev	*Research*
UK	**Royal Holloway, Information Security Group**, Martin Albrecht, Kenny Paterson	*Research, Software, H2020 Grant*
USA	**UC San-Diego, Computer Science Dept.**, Daniele Micciancio	*Research, Software*

Scientific Publications

Bibliometry

Peer-reviewed publications: 34 **H-index: 24** **Citations: 3918**, *according to Google Scholar*

Pre-Prints

2020	**An Algorithmic Reduction Theory for Binary Codes: LLL and more**, Thomas Debris-Alazard, Léo Ducas, Wessel P.J. van Woerden	*Pre-Print*
2020	**Advanced Lattice Sieving on GPUs, with Tensor Cores**, Léo Ducas, Wessel P.J. van Woerden, Marc Stevens	*In Submission*

Peer-Reviewed Publications

2020	**Mildly short vectors in cyclotomic ideal lattices in quantum polynomial time**, Ronald Cramer, Léo Ducas, Benjamin Wesolowski	*Journal of the ACM (To Appear)*
	Random Self-reducibility of Ideal-SVP via Arakelov Random Walks, Koen de Boer, Léo Ducas, Alice Pellet-Mary, Benjamin Wesolowski	*Crypto*
	LWE with Side Information: Attacks and Concrete Security Estimation, Dana Dachman-Soled, Léo Ducas, Huijing Gong, Mélissa Rossi	*Crypto*
	The randomized slicer for CVPP: sharper, faster, smaller, batchier, Léo Ducas, Thijs Laarhoven, Wessel P.J. van Woerden	*PKC*
	On the Quantum Complexity of the Continuous Hidden Subgroup Problem, Koen de Boer, Léo Ducas, Serge Fehr	*Eurocrypt*
	Integral Matrix Gram Root and Lattice Gaussian Sampling without Floats, Léo Ducas, Steven Galbraith, Thomas Prest, Yang Yu	*Eurocrypt*
2019	**On the Shortness of Vectors to be found by the Ideal-SVP Quantum Algorithm**, Léo Ducas, Maxime Plançon, Benjamin Wesolowski	*Crypto*
	The General Sieve Kernel and New records in Lattice Reduction, Martin R. Albrecht, Léo Ducas, Gottfried Herold, Elena Kirshanova, Eamonn W. Postlethwaite, Marc Stevens	*Eurocrypt*
2018	**Learning strikes again: the case of the DRS signature scheme**, Léo Ducas, Yang Yu	*Asiacrypt*
	On the Statistical Leak of the GGH13 Multilinear Map and some Variants, Léo Ducas, Alice Pellet–Mary	*Asiacrypt*
	Polynomial Time Bounded Distance Decoding near Minkowski's Bound in Discrete Logarithm Lattices, Léo Ducas, Cécile Pierrot	*Design, Codes and Cryptography*
	Large FHE Gates from Tensored Homomorphic Accumulators, Guillaume Bonnoron, Léo Ducas, Max Fillinger	*Africacrypt*
	Shortest Vector from Lattice Sieving: A Few Dimension for Free, Léo Ducas	*Eurocrypt*
	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	*Euro S&P*
	CRYSTALS – Dilithium: digital signatures from module lattices, Léo Ducas, Tancrède Lepoint, Vadim Lyubashevsky, Peter Schwabe, Gregor Seiler, Damien Stehlé	*CHES*
	Hash Proof Systems over Lattices Revisited, Fabrice Benhamouda, Olvier Blazy, Léo Ducas, Willy Quash	*PKC*
2017	**Second Order Statistical Behavior of LLL and BKZ**, Léo Ducas, Yang Yu	*Published at SAC*
	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*
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*
	A subfield lattice attack on overstretched NTRU assumptions, Martin Albrecht, Shi Bai and Léo Ducas	*Crypto*
	Fast Fourier Orthogonalization, Léo Ducas and Thomas Prest	*ISSAC*
	Post-Quantum Key Exchange – A New Hope, Erdem Alkim, Léo Ducas, Thomas Poeppelmann and Peter Schwabe	*USENIX security*
	Sanitization of FHE Ciphertexts, Léo Ducas and Damien Stehlé	*Eurocrypt*
	New directions in nearest neighbor searching with applications to lattice sieving, Anja Becker, Léo Ducas, Nicolas Gama and Thijs Laarhoven	*SODA*
	Recovering Short Generators of Principal Ideals in Cyclotomic Rings, Ronald Cramer, Léo Ducas, Chris Peikert and Oded Regev	*Eurocrypt*
	FHEW: Bootstrapping Homomorphic Encryption in less than a second, Léo Ducas and Daniele Micciancio	*Eurocrypt*
2014	**Efficient Identity-Based Encryption over NTRU Lattices**, Léo Ducas and Vadim Lyubashevsky and Thomas Prest	*Asiacrypt*
	Improved Short Lattice Signatures in the Standard, Léo Ducas and Daniele Micciancio	*Crypto*
	Enhanced Lattice-Based Signatures on Reconfigurable Hardware, Thomas Pöppelmann and Léo Ducas and Tim Güneysu	*CHES*

2013	**Lattice Signatures and Bimodal Gaussians**, Léo Ducas and Alain Durmus and Tancrède Lepoint and Vadim Lyubashevsky	*Crypto*
2012	**Learning a Zonotope and More: Cryptanalysis of NTRUSign Countermeasures**, Léo Ducas and Phong Nguyen	*Asiacrypt*
	Faster Gaussian Lattice Sampling using Lazy Floating-Point Arithmetic, Léo Ducas and Phong Nguyen	*Asiacrypt*
	Ring-LWE in Polynomial Rings, Léo Ducas and Alain Durmus	*PKC*
2010	**Anonymity from Asymmetry: New Constructions for Anonymous HIBE**, Léo Ducas	*CT-RSA*