Simon Abelard

Researcher in cryptology at Thales Group

✉ *sabelard@protonmail.com*
sabelard-research.github.io

Current and previous positions

2021- Cryptologist at Thales SIX GTS.

2019-2020 Postdoctoral researcher at École Polytechnique.

2018-2019 Postdoctoral fellow at University of Waterloo (Ontario).

2015-2018 PhD candidate at Université de Lorraine.

Publications

Journal papers

2022 **Efficient computation of Riemann-Roch spaces for plane curves with ordinary singularities.**
With A. Couvreur and G. Lecerf, *Applicable Algebra in Engineering, Communication and Computation*, available on HAL: https://hal.inria.fr/hal-03110135.

2022 **Computing Riemann-Roch spaces via Puiseux expansions.**
With E. Berardini, A. Couvreur et G. Lecerf, *Journal of Complexity*, available on HAL: https://hal.inria.fr/hal-03281757.

2020 **Counting points on hyperelliptic curves with explicit real multiplication in arbitrary genus.** *Journal of Complexity*, available on arxiv : https://arxiv.org/abs/1810.11068 or on the journal's website https://www.sciencedirect.com/science/article/pii/S0885064X19300810.

2018 **Improved complexity bounds for counting points on hyperelliptic curves.**
With P. Gaudry et P.-J. Spaenlehauer, *Foundations of Computational Mathematics*, available on arxiv https://arxiv.org/abs/1710.03448 or on the journal's website https://link.springer.com/article/10.1007/s10208-018-9392-1.

Proceedings of conferences

2020 **Sub-quadratic time for Riemann-Roch spaces. The case of smooth divisors over nodal projective curves.**
With A. Couvreur et G. Lecerf, Proceedings of ISSAC 2020, available here https://dl.acm.org/doi/10.1145/3373207.3404053 or on HAL: https://hal.inria.fr/hal-02477371.

2020 **On the complexity of computing integral bases.**
Proceedings of CASC 2020, available https://dx.doi.org/10.1007/978-3-030-60026-6_3 or on HAL: https://hal.inria.fr/hal-02477371.

July 2018 **Counting Points on Genus-3 Hyperelliptic Curves with Explicit RM.**
With P. Gaudry et P.-J. Spaenlehauer, pp. 1–19 in Proceedings of ANTS XIII. Available on arxiv: https://arxiv.org/abs/1806.05834.

Software

2018 Implementation with P. Gaudry and P.-J. Spaenlehauer of the genus-3 point couting algorithm presented at ANTS XIII. The code used in order to achieve our point-counting record is available here: https://members.loria.fr/SAbelard/RMg3.tgz.

Awards

2019 Thesis prize of the Université de Lorraine.

Seminars and talks

Invited talks

July 2019 **Minisymposium of the international conference SIAM AAG 2019.**
Hyperelliptic point-counting in genus 3 and higher: the RM case.

July 2017 **Minisymposium of the international conference SIAM AAG 2017.**
New complexity bounds for hyperelliptic point-counting.

Talks at national events

Nov. 2020 **Journées Codage et Cryptographie (national French event) 2020.**
Un algorithme (plus) rapide pour calculer des espaces de Riemann-Roch.

March 2020 **Journées nationales du calcul formel (national French event) 2020.**
Calcul de bases intégrales dans des corps de fonctions.

January 2018 **Journées nationales du calcul formel (national French event) 2018.**
Comptage de points de courbes hyperelliptiques en genre 3 et au-delà.

Invitations and seminars

Feb. 2021 Team Polsys seminar, LIP6, Paris

October 2020 Team GRACE seminar, LIX, Palaiseau

July 2020 Team MAX seminar, LIX, Palaiseau

May 2020 Team MAX seminar, LIX, Palaiseau

March 2020 Computer Algebra group seminar, XLIM, Limoges

January 2020 Effective Algebra and Geometry, IRMAR seminar, Rennes.

Nov. 2019 Team GRACE seminar, LIX, Palaiseau.

April 2017 **Three-week invitation at the University of Waterloo.**
One week with Alfred Menezes and David Jao, two weeks with Éric Schost.

Student mentoring and supervision

PhD students

2022-2025 **Algebraic approaches for the cryptanalysis of post-quantum signature schemes**
After obtaining funding from Thales and the French ANRT, I co-supervise a PhD student, jointly with Mohab Safey El Din from Sorbonne Université.

Master internships

2023 **Implementation and study of the Bernstein-Yang constant-time Euclidean algorithm, application to the postquantum candidate BIKE**
A six-month internship of a student in second year Master from Rennes University.

2022 **Computing isogenies: an approach by solving polynomial systems**
A six-month internship of a student in second year Master from Paris-Saclay Uni.

2022 **Side-channel attacks using unsupervised learning**
A six-month internship of a student in second year Master from Sorbonne Université, jointly with ANSSI and a Thales expertise center based in Toulouse.

Teaching

Introductory Mathematics for Cryptography at Telecom Paris

Fall 2020 **Lectures for Master students**
I gave 10 hours of lectures to ∼25 students on mathematical foundations of cryptography (integers, groups, polynomials and finite fields). I designed 5 exercise sheets and an exam that I also marked.

Algorithms and data structures at UWaterloo

Spring 2019 **Lectures for second-year students**
I gave 30 hours of lectures to ∼60 students on introductory computer science (design and complexity analysis of algorithms and various data structures: trees, heaps, queues, etc.). I designed 5 assignments and two exams, and held weekly office hours.

Operations research at Mines Nancy

2017 **Exercise sessions for first-year students**
One group for ∼15h, linear programming (simplex, duality, ILP), with a bit of graphs (shortest path, maxflow) and modelization.

2015 & 2016 **Exercise sessions for second-year students**
Two groups each year, for a total of ∼80h. Content includes graphs (shortest path, maxflow), linear programming (simplex, duality) and convex optimization, with an important focus on modelization.

2016 **Course and exercises for first-year students**
One group for ∼25h, mainly linear programming (simplex, duality, sensitivity analysis), with a bit of graphs and modelization.

Computer science at Mines Nancy

2018 **Algorithmics and programming for first-year students**
Exercise sessions in Python for ∼20h.

2016 & 2017 **Algorithmics and programming for second-year students**
Exercise sessions in Python, for a total of ∼35h.

2017 **Data bases for second-year students**
Exercise sessions (relational algebra, normal forms and queries in SQL), for ∼20h.

Academic duties

2022 Review for the international conference ISSAC.

2022 Review for a special issue of the Journal of Complexity.

2021 Jury member for the PhD defense of Mohammed Zitouni (Université Paris 8).

2021 Review for the international conference ISSAC.

2020 Review for the journal AAECC (Applicable Algebra in Engineering, Communication and Computing).

2020 Review for the international conference Africacrypt.

2019 Review for a special issue of the journal AAECC dedicated to Algebraic Geometry from an algorithmic point of view.

2019-2021 Evaluation of applications to the Bachelor program of École Polytechnique (about 300 applications in total).

2019-2020 Proofread a book chapter for the "École jeunes chercheurs en Informatique-Mathématiques".

2016 Review for the international conference SAC 2016 (Selected Areas in Cryptography).

Popularization

Nov. 2019 Entretiens de l'Excellence: I spent two afternoons with highschool students to present them scientific studies and careers.

Education

2015–2018 **Ph.D. in computer science**, *Université de Lorraine*, Nancy.
Supervised by Pierrick Gaudry and Pierre-Jean Spaenlehauer: *Counting points on hyperelliptic curves in large characteristic: algorithms and complexity*.
The committee was composed of: Guillaume Hanrot (president)
Christophe Ritzenthaler and Fréderik Vercauteren (referees)
Magali Bardet and Elisa Gorla (examiners)

2014–2015 **Master's degree, *Agrégation***, *ENS Cachan*, *Summa cum laude*.
One-year preparation to the French *Agrégation*.

2013–2014 **Master's degree**, *Université Pierre et Marie Curie*, Paris, *Cum laude*.
Degree in pure Mathematics, majoring in Number Theory and Algebraic Geometry

2012–2013 **Second year at ENS**, *ENS Cachan*, *Summa cum laude*.
General courses in Mathematics, with a five month research experience

2011–2012 **Bachelor**, *Université Paris VII Diderot, ENS Cachan*, *Cum laude*.

Computer skills

Engineering IBM DOORS

CAS Magma, Maple

Technical Matlab, Scilab, AMPL

Programming C, Python