Dr. Tako Boris Fouotsa

Postdoctoral Researcher

INF 235, Station 14
1015 Lausanne, Switzerland
+41 77 275 69 42
+41 21 693 81 27
tako.fouotsa@epfl.ch
www.borisfouotsa.com
Date: March 2024

Research interests

- Isogeny-based cryptography (design and cryptanalysis);
- Post-quantum cryptography cryptanalysis;
- Advanced protocols;
- Applied cryptography;
- Classical cryptography cryptanalysis (integer factorisation and discrete logarithm problem).

Positions

03.2022 - ... **Postdoctoral Researcher**, *Cryptography and Security Lab (LASEC), EPFL*, Switzerland

02.2022 **Research Assistant**, *School of Computer Science*, University of Birmingham, UK

Education

02.2022 **PhD in Isogeny-Based Cryptography**, *University of Roma Tre*, Italy

2017 **Msc degree in Mathematics**, *University of Yaoundé I*, Cameroon

2016 **Diplôme de Professeur de l'Enseignement Secondaire 2eme Grade (DiPES II) en Mathématiques**, *École Normale Supérieure de Yaoundé*, Cameroon, Overall second best student

2014 **Bachelor's Degree in Mathematics**, *University of Yaoundé I*, Cameroon

2014 **Diplôme de Professeur de l'Enseignement Secondaire 1er Grade (DiPES I) en Mathématiques**, *École Normale Supérieure de Yaoundé*, Cameroon, Overall best student

Professional experience

Research visits
- ENS Lyon, March 2024.
- LFANT, Institut de Mathématiques de Bordeaux, May 2023.
- IRMAR Rennes, Dec 2022;
- Cybersecurity Research Center, Universite Libre de Bruxelles, September 2022;
- IBM Zurich, July 2022;

Research stays
- University of Bamenda, July-October 2021;
- University of Bamenda, August 2020;
- University of Birmingham's School of Computer Science, March-July 2020;
- University of Bamenda, August-October 2019.

Steering Committee
- Master/PhD Program in Cybersecurity and Cryptology at the University of Bamenda, Cameroon. The first 5 years of the Master program are funded by ARES Belgique.

General (co-)Chair
- AFRICACRYPT 2024, Douala, Cameroon, 10-12 July, 2024.

Program Committee

- FCiR 2025, Rome, Italy, 1st October, 2025.
- AFRICACRYPT 2025, Rabat, Morocco, 21-23 July, 2025.
- PQCrypto 2025, Taipei Taiwan, 8-10 April 2025.
- CIFRIS 2024, Rome, Italy, 27-29 September, 2024.
- AFRICACRYPT 2024, Douala, Cameroon, 10-12 July, 2024.
- ACNS 2024, New York University Abu Dhabi Campus, U.A.E., 5-8 March 2024.
- ANTS XV, University of Bristol, 08-12 August, 2022.

Reviewing services

- Eurocrypt 2023, 2024, 2025;
- ACISP 2025;
- ESORICS 2025;
- CANS 2024;
- PKC 2021, 2023;
- C2SI 2023;
- IMACC 2021;
- Inscrypt 2021;
- PQCrypto 2021;
- Journal of Cryptology
- Designs, Codes and Cryptography
- Mathematical Cryptology
- IET Information Security journal;
- IEEE Access journal;

Teaching

- 27.01.2025 - 15.02.2025: Cryptography course at AIMS Cameroon, Teaching Assistant and Substitute Lecturer.
- 2024/2025: Post-Quantum Cryptography, Fall 2024, University of Bamenda, online course.
- 2024/2025: Cryptography and Security, Fall 2024, IC School, EPFL. Substitute Lecturer.
- 2023/2024: Advanced Cryptography, Spring 2024, IC School, EPFL. Substitute Lecturer.
- 29.01.2024 - 17.02.2024: Cryptography course at AIMS Cameroon, Teaching Assistant and Substitute Lecturer.
- 2023/2024: Cryptography and Security, Fall 2023, IC School, EPFL. Substitute Lecturer.
- 21.08.2023 - 25.08.2023: Mon premier pas vers la cryptographie, summer school course at Lycée Général Leclerc, Yaoundé Cameroon.
- 2022/2023: Cryptography and Security, Fall 2022, IC School, EPFL. Substitute Lecturer.
- 2021/2022: Advanced Cryptography, Spring 2022, IC School, EPFL. Substitute Lecturer.

PhD mentoring

- January 2024 - Now: Max Duparc, PhD student in Post-Quantum Cryptography, EPFL, Switzerland;
- July 2021 - Now: Tchoffo Saah Gustave, PhD student in Isogeny-based Cryptography, University of Yaounde I, Cameroon;

Master Thesis supervision
- Spring 2025: Simon Olivier Paul Laude, EPFL Switzerland; *Verifiable Random Functions and their use in practice: the case of Algorand.*
- Spring 2025: Jean Gabriel Agapka Vigno, AIMS Cameroon, *Class group computation.*
- Spring 2025: Mohammed Yusuf, University of Bamenda, Cameroon, *MEDS Post-Quantum Digital Signature.*
- Spring 2025: Laila Rene, University of Bamenda, Cameroon, *LESS Post-Quantum Digital Signature.*
- Spring 2025: Bolabo Obase, University of Bamenda, Cameroon, *MAYO Post-Quantum Digital Signature.*
- Fall 2023: Max Duparc, Msc student at EPFL; *Isogeny Based Updatable Public Key Encryption Schemes.*
- Spring 2023: Vincent Gali Ehba, AIMS Cameroon, *The Elliptic Curve factorisation Method.*

Semester Projects
- Spring 2025: Adrián Saiz De Pedro, EPFL Switzerland; *Anonymous Credentials from ECDSA.*
- Spring 2025: Octave Eiji Charrin, EPFL Switzerland; *Exotic Post-Quantum Signatures for Blockchain.*
- Fall 2024: Yuchen Chang, Msc student at ETH, semester project on *Anamorphic Encryption.*
- Spring 2024: Parsa Tasbihgou, Msc student at EPFL, semester project on *Isogeny Based Delay Encryption.*
- Spring 2023: Malo Ranzetti, Msc student at EPFL, semester project on *Countermeasures to SIDH attacks.*
- Spring 2023: Alessandro Colombo, Msc student at EPFL; semester project on *Using supersingular curves and anomalous curves in ECM.*

Summer interns at EPFL
- Summer 2023: Amer Elsheikh, The American University in Cairo, Egypt. *An Elliptic Curve Based Symmetric Encryption scheme.*
- Summer 2023: Mohammadreza Motabar, University of Tehran, Iran. *On the Number Field Sieve Factoring Method.*

Course tutoring
- Summer course on linear algebra, John Cabot University of Rome, June 2019;
- Nepal Algebra Project, Tribhuvan University Nepal, May-July 2019 (remote).

High school Mathematic Teacher
- Goverment Bilingual High School Nanga-Eboko, Centre, Cameroon; January 2017 - December 2018.
- Academic College of Excellence, Yaounde, Centre, Cameroon; October 2016 - June 2018.
- Goverment Bilingual High School Etoug-Ebe, Centre, Cameroon; January 2016 - May 2016.
- Lycee Technique Industriel et Commercial Yaounde, Centre, Cameroon; January 2014 - May 2014.

Volunteering

03.2023 - ... Animatheurs at Animath

August 2023 Invited teacher at a Mathematical summer school for high school students in Yaoundé, with the support of the Animath association.

04.2023 - 03.2024 Vice President of Innovation Forum Lausanne

July 2021 Member of the early stage researcher organising committee of EMA (Ecole de Mathematiques Africaine) School Dschang, University of Dschang.

July 2018 Member of the early stage researcher organising committee of EMA (Ecole de Mathematiques Africaine) School Yaounde, University of Yaounde I.

Languages

Working *English*, *French*.

Fluent *Italian* (B2), *Ngiemboon* (native language).

Beginner German (A2).

Other Skills

Software skills LaTeX, Sagemath, Python, Microsoft package

Soft skills Fast adaptation, Quick learner, Leadership, Negotiation, Communication

Projects

SQISign [Webpage] Highly compact isogeny-based post-quantum signature scheme submitted to the second round of NIST's second call for post-quantum digital signatures [link].

Publications (Google scholar profile: link)

- T. Decru, T. B. Fouotsa, P. Frixons, V. Gilchrist and C. Petit, *Attacking trapdoors from matrix products*. Accepted for the IACR Communications in Cryptology, Volume 1, Issue 3. Eprint
- ★ M. Duparc, T. B. Fouotsa, *SQIPrime: A dimension 2 variant of SQISignHD with non-smooth challenge isogenies*. Accepted at ASIACRYPT 2024 [Honorable mention]. Eprint
- M. Duparc, T. B. Fouotsa, S. Vaudenay, *SILBE: an Updatable Public Key Encryption Scheme from Lollipop Attacks*. Accepted at SAC 2024. Eprint
- J. Booher, R. Bowden, J. Doliskani, S. D. Galbraith, T. B. Fouotsa, S. Kunzweiler, S.-P. Merz, C. Petit, B. Smith, K. E. Stange, Y. B. Ti, C. Vincent, J. F. Voloch, C. Weitkämper, and L. Zobernig, *Failing to hash into supersingular isogeny Graphs*. Full paper to appear at The Computer Journal. Eprint.
- L. De Feo, T. B. Fouotsa, L. Panny, *Modular Isogeny Problems*. Accepted at EUROCRYPT 2024. Eprint.
- A. Basso, M. Chen, T. B. Fouotsa, P. Kutas, A. Laval, L. Marco, G. T. Saah, *Exploring SIDH-based Signature Parameters*. Published at ACNS 2024. Paper Eprint.
- ★ A. Basso and T. B. Fouotsa, *New SIDH Countermeasures for a More Efficient Key Exchange*. Published at ASIACRYPT 2023. Paper Eprint.
- ★ T. B. Fouotsa, T. Moriya and C. Petit, *M-SIDH and MD-SIDH: countering SIDH attacks by masking information*. Published at EUROCRYPT 2023. Paper Eprint.
- A. Basso, G. Codogni, D. Connolly, L. De Feo, T. B. Fouotsa, G. M. Lido, T. Morrison, L. Panny, S. Patranabis, B. Wesolowski, *Supersingular Curves You Can Trust*. Published at EUROCRYPT 2023. Paper Eprint.
- ★ L. De Feo, T. B. Fouotsa, P. Kutas, A. Leroux, S.-P. Merz, L. Panny and B. Wesolowski, *SCALLOP: scaling the CSI-FiSh*. Published at PKC 2023. Paper Eprint.
- J. Booher, R. Bowden, J. Doliskani, S. D. Galbraith, T. B. Fouotsa, S. Kunzweiler, S.-P. Merz, C. Petit, B. Smith, K. E. Stange, Y. B. Ti, C. Vincent, J. F. Voloch, C. Weitkämper, and L. Zobernig, *Failing to hash into supersingular isogeny Graphs*. Extended abstract published at CFAIL 2022. Eprint.
- ★ T. B. Fouotsa and P. Kutas and S.-P. Merz, *On the isogeny problem with torsion points*. Published at PKC 2022 [Invitation to the Journal of Cryptology (equivalent to best paper award)]. Paper Eprint.
- T. B. Fouotsa and C. Petit, *A New Adaptive attack on SIDH*. Published at CT-RSA 2022. Paper Eprint.
- T. B. Fouotsa and C. Petit, *SHealS and HealS: Isogeny-Based PKEs from a Key Validation Method for SIDH*. Published at ASIACRYPT 2021. Paper Eprint
- L. De Feo, C. D. de Saint-Guilhem, T. B. Fouotsa, A. Leroux, P. Kutas, C. Petit, J. Silva and B. Wesolowski, *SETA: Supersingular Encryption from Torsion point Attacks*. Published at ASIACRYPT 2021. Paper Eprint.

- T. B. Fouotsa and C. Petit, *SimS: A simplification of SiGamal*. Published at PQCrypto 2021. Paper Eprint.

In Submission

- G. T. Saah, T. B. Fouotsa, E. Fouotsa, C. Nkuimi-Jugnia, *Avoiding Trusted Setup in Isogeny-based Commitments*, Eprint.
- P. Dartois, J. K. Eriksen, T. B. Fouotsa, A. Herlédan Le Merdy, R. Invernizzi, D. Robert, R. Rueger, F. Vercauteren, B. Wesolowski, *PEGASIS: Practical Effective Class Group Action using 4-Dimensional Isogenies*, Eprint.

Preprints

- Tako Boris Fouotsa, *A note on the prime in SQISignHD*. Draft.
- Tako Boris Fouotsa, *SIDH with masked torsion point images*. Eprint.

Attended Events

Conferences Africacrypt 2024, Eurocrypt 2024, SIAM AG 23, Eurocrypt 2023, AfricaCrypt 2022, Leuca 210, CT-RSA 2022, Asiacrypt 2021, Eurocrypt 2021, Crypto 2021, PQCrypto 2021, Third NIST PQC Standardization Conference (June 7-9 2021), PKC 2021, RWC 2021, Asiacrypt 2020, SAC 2020, PQCrypto 2020, Crypto 2020, ANTS-XIV, PKC 2020, Eurocrypt 2020, ITASEC20, PQCrifis e CifrisChain 2019, RNTA 5th Mini Symposium 2019.

Workshops Swissogeny days (Jan 21st, 2025 EPFL), Leuven Isogeny Days 5 (Sept 11 - 13, 2024 KU Leuven), Isogeny Club Brainstorm Days, Eurocrypt 2024 (May 25 - 26, 2024 ETH Zurich), Quantum Safe Workshop (May 24, 2024, IBM Research Zurich), Leuven Isogeny Days 4 (Oct 11 - 13, 2023 KU Leuven), Isogeny Club Brainstorm Days, Eurocrypt 2023 (May 22 - 23, 2023 ENS Lyon), Leuven Isogeny Days 3 (Sept 21 - 23, 2022 KU Leuven), Summer School in post-quantum cryptography (August 1-5 2022 Budapest), An ordinary day in supersingularland (July 07 2022 IBM Research Zurich), Banff isogeny workshop (August 22 to August 27, 2021) on Supersingular isogeny graphs in cryptography, SAC 2020 workshop, NIST NCCoE workshop 7 October 2020, ANTS-XIV's workshop, 13th Pari/GP Atelier april 2019, 21^{st} Workshop on Algebra and Logic Yaounde August 2017.

Schools Digital CISPA summer school on Coding Techniques and Advanced Post-Quantum Cryptography (Online August 30-Sept 03 2021), Bristol's Isogeny-based cryptography school (Online July-Sept 2021), EMA and CRAG-10 Dschang 2021 (19th - 30th July 2021), ANTS-XIV's summer school, CIMPA School Limbe July 2019, EMA School Yaounde July 2018, CIMPA School Kinshasa May 2018.

Talks

Sept. 2024 *SQIPrime*, Leuven Isogeny Days 5, KU Leuven, Belgium.

May 2024 *Isogeny Problems with Level Structure*, Eurocrypt 2024, Zürich, Switzerland. Slides Video (39:00 →)

Apr. 2024 *Recovering isogenies from a single torsion point image, and more.* ACCESS: Algebraic Coding and Cryptography Seminar Series. Slides

Dec. 2023 *Isogeny Representations and their Applications to Cryptography*, University of Neuchatel, Neuchatel, Switzerland. Abstract and video.

Oct. 2023 *A look at SQISignHD*, Leuven Isogeny Days 4, KU Leuven, Belgium. Slides

July 2023 *At the evening of SIDH attacks*, "Applications of algebraic geometry to post-quantum" cryptology Symposium, co-located with SIAM AG23, Eindhoven, The Netherlands.

May 2023 *Beyond the SIDH Countermeasures*, LFANT, Institut de Mathématiques de Bordeaux.

April 2023 *M-SIDH and MD-SIDH: countering SIDH attacks by masking information*, Eurocrypt 2023, Lyon, France.

Dec. 2022 *On the countermeasures to the higher genus torsion point attacks on SIDH*, Séminaire de Cryptographie de Rennes, IRMAR, Universite de Rennes. Slides

Nov. 2022 *Torsion point images in SIDH: from savior to killer*, Isogeny club presentation. Slides

Sep. 2022 *Masking SIDH: where do we stand?*, Leuven isogeny days, September 21st-23rd 2022. Slides

July 2022 *A New Adaptive Attack on SIDH*, IBM Zurich. Slides

March 2022 *A New Adaptive Attack on SIDH*, CT-RSA 2022.

Dec. 2021 *SHealS and Heals: isogeny-based PKEs from a key validation method for SIDH*, Asiacrypt 2021.

Dec. 2021 *SETA: Supersingular Encryption from Torsion points Attack*, Asiacrypt 2021 (5 min presentation).

Oct. 2021 *A closer look at the torsion points in SIDH*, hiring talk at LASEC, EPFL.

July 2021 *SETA: Supersingular Encryption from Torsion points Attack*, CRAG-10.

July 2021 *SimS: A Simplification of SiGamal*, PQCrypto 2021.

June 2021 *SimS: A Simplification of SiGamal*, Cryptography Seminar, University of Roma Tre.

August 2020 *An overview of SIDH*, MaC Seminars, Cameroon.

August 2020 *An overview of CSIDH*, MaC Seminars, Cameroon.

Dec. 2019 *An introduction to Isogeny-Based Cryptography*, Mathematic PhD seminars, University of Roma Tre.

July 2019 *Dirichlet's Units Theorem*, CIMPA School, African Institute for Mathematical Science (AIMS) Limbe

Scholarships and Honours

2024 Honorable mention at ASIACRYPT 2024.

May 2024 1st Bridge Africa Summit/Program, UM6P, Ben Guerir, Morocco. A platform where Young African Leaders can acquire leadership skills that will enable them to further impact their communities.

2022 Con Lode grade (highest distinction) for my PhD work, University of Roma Tre, Italy.

2022 Invitation to the Journal of Cryptology at PKC 2022 (equivalent to best paper award).

2018-2021 PhD scholarship at the University of Roma Tre, Italy

2016 Second best student of the second cycle Mathematics 55th batch of ENS Yaounde

2014 Best student of the first cycle Mathematics 53rd batch of ENS Yaounde

Other Research Community Activities

January 2025 Initiator and host of the first edition of *Swissogeny days*, a recurrent isogeny-based cryptography workshop that gathers isogenists from all over Switzerland. The first edition is scheduled for January 21st 2025 at EPFL.

August 2020 Co-initiator (with Pr. Emmanuel Fouotsa of the University of Bamenda) of the MaC (Mathematics and Cryptology) Seminars in 2020. These are online seminars held by Cameroonian (professionals and early stage) researchers working on Cryptography and related topics. We are currently preparing a web webpage for these seminars.

2019 "Scriba" editor, Roman Number Theory Association (RNTA) 5th mini symposium 2019.

2020 - Now Member of the International Association for Cryptologic Research (IACR).