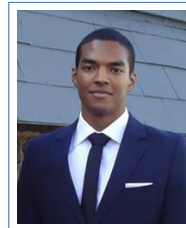


Jérôme Govinden

PhD Candidate in Cryptography

+49 (0)176 40797051
jerome@jeromegovinden.com
jeromegovinden.com
in jeromegovinden
French and Mauritian nationality



Professional Experience

- 2020–Present **Research Assistant in the Cryptography and Network Security (CNS) group**
Technische Universität Darmstadt - Darmstadt, Germany
- 2024 **Research Intern in the Cryptography Research Group**, working with Stefano Tessaro, on designing fast condensers and pseudorandom number generators
University of Washington - Seattle, WA, USA
- 2022–2023 **Research Intern in the Cryptography Research Center (CRC)**, working with Jean Paul Degabriele, on new polynomial hash designs and their efficient implementation
Technology Innovation Institute - Abu Dhabi, UAE
- 2018–2019 **Cryptology & Security Engineer**
Master Data Solutions - Paris, France
- 2015–2016 **Consultant in Multivariate Cryptography**
Satt Lutech/Laboratoire d'informatique de Paris 6 (LIP6) - Paris, France
- 2015 **Research Intern in the PolSys Team**, working with Jean-Charles Faugère and Ludovic Perret, on symbolic computation and multivariate cryptography
Laboratoire d'informatique de Paris 6 (LIP6), Sorbonne Université - Paris, France
- 2014 **Application Analyst Intern and Assistant Project Manager**
Mauritius Commercial Bank (MCB) Consulting Services Ltd. - Port-Louis, Mauritius

Educational Background

- 2020–Present **PhD Candidate in Cryptography**, Technische Universität Darmstadt, Darmstadt, Advisor: Jean Paul Degabriele
Current research interest: universal hash functions, randomness extraction, efficient design, analysis and implementation of provably secure schemes
- 2018–2019 **Master of Science in Mathematics and Applications**, Université Paris Diderot, Paris
With specialization in Mathematics, Computer Science and applications to Cryptology (MIC), highest honors
- 2014–2015 **Master of Science in Computer Science**, Université Pierre et Marie Curie, Paris
With specialization in Digital Security, Reliability and Performance (SFPN)
Master thesis: Design of a root finding algorithm for sparse polynomials and analysis of its applications in finite fields
- 2011–2012 **Bachelor of Science in Mathematics**, Université Pierre et Marie Curie, Paris
- 2009–2011 **Preparation for the competitive entrance to French Engineering Schools**, Lycée Saint-Louis, Paris
Main topics: mathematics, physics, chemistry and computer science
- 2009 **High School Diploma in Sciences**, Lycée La Bourdonnais, Curepipe, Mauritius
With highest honors

Skills

Computer Science

- Programming C (GMP), C++, C#, Python, parallel programming (OpenMP, MPI, CUDA), Script Shell
- Computer algebra Magma, Sage, Maple, Matlab
- Networks Networks architecture, OSI model, QOS, digital transmission systems and errors analysis, mobile web and network standards, routing protocols, DHCP, transport layer protocols: TCP et UDP, ssh, DNS, HTTP, FTP
- Security Efficient implementations and attacks of cryptographic algorithms (AES, RSA, ECDH, ECDSA, SHA), side channel attacks, cryptographic protocols (TLS, IPSEC), standards (PKCS, RFC, NIST, FIPS, ISO, ANSSI), PKI
- Others Modeling, designing and efficient implementation of algorithms

Mathematics

- Algebra Polynomial system solving, linear algebra, algebraic number theory, Galois theory
- Cryptography Algebraic cryptography, multivariate cryptography, lattice theory, elliptic curves, factorization, primality test
- Others Floating point arithmetic, topology, measure theory, differential calculus, probability, holomorphic function


Language

French: Mother tongue

English: Fluent

German: Moderate

Projects

- 2021–Present **Benchmarking framework for polynomial-based universal hash functions**,  git repository
Developed modular implementations achieving performance competitive with state-of-the-art universal hash functions.
The new design Poly1163 achieves up to 40% speedup compared to Poly1305 while maintaining the same security.
- 2019 (5 months) **Implementations of LFSR (A5/1, Berlekamp-Massey), a polynomial library and differential cryptanalysis**
- 2015 (4 months) **Implemented cryptographic algorithms for JavaCard and side channel attacks using ChipWhisperer**

Publications

Conferences with Proceedings (peer reviewed)

Joël Alwen, Chris Brzuska, Jérôme Govinden, Patrick Harasser, and Stefano Tessaro. Succinct PPRFs via Memory-Tight Reductions. In *Advances in Cryptology – CRYPTO 2025*. Springer-Verlag, 2025.

Ritam Bhaumik, Bishwajit Chakraborty, Wonseok Choi, Avijit Dutta, Jérôme Govinden, and Yaobin Shen. The Committing Security of MACs with Applications to Generic Composition. In *Advances in Cryptology – CRYPTO 2024*. Springer-Verlag, 2024.

Jean Paul Degabriele, Jan Gilcher, Jérôme Govinden, and Kenneth G Paterson. SoK: Efficient Design and Implementation of Polynomial Hash Functions over Prime Fields. In *2024 IEEE Symposium on Security and Privacy (SP)*, pages 132–132. IEEE Computer Society, 2024.

Jean Paul Degabriele, Marc Fischlin, and Jérôme Govinden. The Indifferentiability of the Duplex and Its Practical Applications. In *International Conference on the Theory and Application of Cryptology and Information Security (Asiacrypt 2023)*, pages 237–269. Springer, 2023.

Jean Paul Degabriele, Jérôme Govinden, Felix Günther, and Kenneth G Paterson. The Security of ChaCha20-Poly1305 in the Multi-User Setting. In *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security*, pages 1981–2003, 2021.

Workshops without Proceedings

Jean Paul Degabriele, Jan Gilcher, Jérôme Govinden, and Kenneth G Paterson. Universal Hash Designs for an Accordion Mode. In *NIST Workshop on the Requirements for an Accordion Cipher Mode 2024*, 2024.

Academic Services

- External reviewer ACM CCS (2022, 2023, 2025), CRYPTO (2022, 2023, 2024), EUROCRYPT (2022), CT-RSA (2021, 2022), ACNS (2024), Financial Cryptography (2021)
- Staff member Cryptographic Hardware and Embedded Systems (CHES) 2015

Talks

- CRYPTO 2024 **The Committing Security of MACs with Applications to Generic Composition**, Santa Barbara, CA, USA, 21/05/2024
- S&P 2024 **SoK: Efficient Design and Implementation of Polynomial Hash Functions over Prime Fields**, San Francisco, CA, USA, 21/05/2024
- RWC 2024 **What’s wrong with Poly1305? - Improving Poly1305 through a Systematic Exploration of Design Aspects of Polynomial Hash Functions (joint talk with Jan Gilcher)**, Toronto, Canada, 27/03/2024
- ASIACRYPT 2023 **The Indifferentiability of the Duplex and its Practical Applications**, Guangzhou, China, 08/12/2023
- CCS 2021 **The Security of ChaCha20-Poly1305 in the Multi-User Setting**, virtual, 17/11/2021

Invited Seminars and Workshops

- Nov. 2025 **GelreCrypt 2025**, Nijmegen, Netherlands
- Sep. 2025 **Generic Attacks and Proofs in Symmetric Cryptography**, Singapore
- Dec. 2023 **Asian Workshop on Symmetric-Key Cryptography**, Guangzhou, China

Teaching

- Teaching assistant **Symmetric Cryptography Course by Jean Paul Degabriele**, Technische Universität Darmstadt (2020–2022)
- [Master thesis](#)
- 2025 **Analysis of the symmetric encryption mechanisms in the PDF 2.0 specification**, A. C. T.
- [Bachelor thesis](#)
- 2024 **Performance Analysis of Multilinear Galois Mode and variants**, P. H.
- 2022 **Analysis of the Impact of Dovetail Routing on the Anonymity of the Lightning Network**, C. M., co-supervised with Jean Paul Degabriele