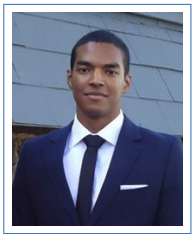
Jérôme Govinden

PhD Candidate in Cryptography

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



Professional Experience

2020-Present **Research Assistant in the Cryptography and Network Security (CNS) group**.
Technische Universität Darmstadt - Darmstadt, Germany

2022-2023 **Research Intern in the Cryptography Research Center (CRC)**.
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 Symbolic Computation and Multivariate Cryptography**.
Laboratoire d'informatique de Paris 6 (LIP6) - 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: provable security with real-world applications, universal polynomial hash, authenticated encryption

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)

2012-2014 **Master of Science (1st Year) in Mathematics and Applications**, *Université Pierre et Marie Curie* - Paris.

Master of Science (1st Year) in Computer Science, *Université Pierre et Marie Curie/Télécom ParisTech* - Paris.
With specialization in computer networks

2011-2012 **Bachelor of Science in Pure 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

Publications

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.

Projects

2021-Present ○ **Benchmarking Framework for Polynomial-Based Universal Hash Functions**, git repository

2019 (5 months) ○ **Implementations of LFSR (A5/1, Berlekamp-Massey), a Polynomial library and differential cryptanalysis**

2015 (4 months) ○ **Programming Cryptographic Algorithms for JavaCard and Side Channel Attacks with ChipWhisperer**

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	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, Privacy
Others	Modeling, Designing and Efficient Implementation of Algorithms

Mathematics

Algebra	Polynomial System Solving, Linear Algebra, Algebraic Number Theory, Galois Theory
Cryptology	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

Academic Services

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

Talks

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.

Teaching

Teaching assistant	**Symmetric Cryptography Course by Jean Paul Degabriele**, *Technische Universität Darmstadt (2020-2022)*.