Diego de Freitas Aranha

Associate Professor at Department of Computer Science, Aarhus University, Denmark
Åbogade 34, 8200 Aarhus N, Aarhus, Denmark.
E-mail: dfaranha@cs.au.dk
Phone: +45 91 88 14 46
Website: https://dfaranha.github.io

Research Objectives

Enable the development of secure computer systems through efficient and robust cryptography, privacy-preserving protocols and lessons from security analysis of real-world systems.

Research Interests

Efficient algorithms and software implementations for symmetric and public key cryptography; privacy-preserving cryptographic protocols; security of real-world systems.

Public Profiles

- ORCID: https://orcid.org/0000-0002-2457-0783
- ResearcherID: https://www.researcherid.com/rid/J-9961-2012
- Google Scholar: https://scholar.google.com/citations?user=FF26-mIAAAAJ
- SCOPUS: https://www.scopus.com/authid/detail.uri?authorId=16041624100
- DBLP: http://dblp.uni-trier.de/pers/hy/a/Aranha:Diego_F=

Education

University of Waterloo, Waterloo, Canada
Visiting PhD student **04/2010 – 04/2011**
- Project: Pairing-Based Cryptography: Theory and Practice
- Advisor: Alfred Menezes
- Area of study: Cryptographic Engineering

University of Campinas, Campinas, Brazil
PhD in Computer Science **03/2007 – 08/2011**
- Thesis: Efficient software implementation of curve-based cryptography
- Advisor: Julio López
- Area of study: Cryptographic Engineering

Master of Computer Science **03/2005 – 02/2007**
- Dissertation: Name services and routing in anonymizing networks
- Advisor: Julio López
- Area of study: Computational anonymity

University of Brasília, Brasília, Brazil
Bachelor of Computer Science **02/2000 – 02/2005**
- Project: An anonymizing transport layer with applications to censorship-resistant services
- Advisor: João Gondim
- Area of study: Computational anonymity

Professional Experience

Aarhus University, Aarhus, Denmark
Associate Professor, Department of Computer Science **08/2020 – Present**
- Researcher on Cryptographic Engineering and Systems Security.
- Lectured courses on Computer Architecture and Network/Systems Security.

Assistant Professor, Department of Engineering **07/2018 – 07/2020**
- Researcher on Cryptographic Engineering and Network Security.
- Lectured courses on Data Structures and Network Security.

University of Campinas, Campinas, Brazil
Assistant Professor, Institute of Computing **02/2014 – 06/2018**
- Researcher on Cryptographic Engineering and Systems Security.
- Lectured undergrads on Algorithms and Computer Programming, Computer Architecture, Assembly Programming, and Competitive Programming.
- Lectured graduate courses on Cryptography, Secure Programming and Algorithm Complexity.

University of Brasília, Brasília, Brazil
Assistant Professor, Department of Computer Science **11/2011 – 02/2014**
- Researcher on PUF-based Cryptography and Electronic Voting.
- Lectured courses on Cryptography, Object-Oriented Programming, Computer Architecture, Competitive Programming, Computational Logic, Systems Software.

CertiVox/MIRACL, London, UK
Contractor/Developer **09/2010 – 11/2011**
- Implemented pairing-based cryptography for secure messaging in C++ and JavaScript.

Honors and Awards

- Distinsguished Program Committee Member at EUROCRYPT 2024 **2024**
- Invited to discuss security issues with electronic voting at Brazilian Senate **2018**
- Defended strong encryption on public hearing at Brazilian Supreme Court **2017**
- Google Research Awards in Latin America for research in privacy **2015/2016**
- Innovators Under 35 Brazil by MIT TechReview for work in electronic voting **2015**
- Raised US$ 30,000 in crowdfunding campaign for YouInspect project **2014**
- Best Paper Award in Cryptographic Hardware and Embedded Systems (CHES) **2013**
- Best PhD dissertation in Brazil on Computer Security and Cryptography **2012**
- 2nd Best Computer Science PhD Thesis in Brazil by Brazilian Computer Society **2012**
- Best PhD dissertation defended in 2011 at Institute of Computing, University of Campinas **2012**
- Invited to discuss security issues with electronic voting at Brazilian Congress **2012**
- 1st place at the 2nd Edition of the Public Security Tests of the Electronic Voting System organized by the Brazilian Electoral Authority **2012**
- Visiting PhD Student Scholarship by CAPES funding agency **2010-2011**
- Prestigious PhD Scholarship by FAPESP funding agency **2007-2010**
- 5th/8th place in South American ACM International Collegiate Programming Contest **2003/2004**

Quantitative indicators

Current supervisions: 1 PhD supervision, 1 PhD co-supervision.

Completed supervisions: 51 undergrad research and final projects, 50 MSc. dissertations (with co-supervisions), 9 PhD theses (with co-supervisions), 1 Postdoc.

Publications: 34 journal articles, 2 edited volumes, 3 book chapters, 60 papers in conference proceedings, 13 papers in peer-reviewed workshops.

Citations: 4050 (Google Scholar), 2140 (ResearchGate), 1467 (Scopus), 879 (ISI).

H-Index: 31 (Google Scholar), 24 (ResearchGate), 20 (Scopus), 15 (ISI).

Funding

Aarhus University, Aarhus, Denmark

MPCC: MPC in the Confidential Cloud (co-PI) **01/2025 – Present**
- Grant: CyberAgentur, DKK 13,000,000
- Objective: Develop efficient quantum-safe algorithms for privacy-preserving computation.

SCI: Secure Computation Infrastructures (PI) **10/2024 – Present**
- Grant: Salling Foundation, DKK 4,800,000
- Objective: Develop MPC and strong authentication solutions for the retail industry.

RENAIS: Residue Number Systems for Cryptography (PI) **07/2021 – Present**
- Grant: Independent Research Fund Denmark, DKK 2,871,000
- Objective: Develop algorithms for high-assurance field arithmetic in RNS representation.

Verifiable cryptographic software (PI) **08/2019 – 12/2022**
- Grant: Partnership with Concordium Blockchain Research Center, DKK 2,250,000.
- Objective: Develop techniques for formal verification of cryptographic software.

BAN – Blockchain Network Academy (PI) **01/2020 – 06/2022**
- Grant: Danish Industry Fund, DKK 1,673,000 for AU within total of 6,750,000 to consortium.
- Objective: Develop training materials and use cases for secure blockchain applications.

Cybersecurity in secure manufacturing (PI) **12/2018 – 10/2020**
- Grant: Partnership with Aerospace & Defence Manufacturing Groupe (ADMAG) in the Smart Industry program, DKK 1,000,000.
- Objective: Prototype and deploy techniques for secure sharing of production data.

University of Campinas, Campinas, Brazil

Privacy-preserving analytics with differential privacy (PI) **04/2018 – 04/2019**
- Grant: Seed funding from LG Electronics, US$ 50,000.
- Objective: Design efficient protocols and implementations satisfying differential privacy.

Efficient and secure cryptography for IoT (PI) **02/2015 – 03/2018**
- Grant: Partnership with LG Electronics, US$ 250,000.
- Objective: Design efficient software implementations for lightweight cryptography.

Machine learning over encrypted data using homomorphic encryption (PI) **10/2015 – 10/2017**
- Grant: Google Research Awards for Latin America, US$ 40,000.
- Objective: Design algorithms and protocols for machine learning tasks over encrypted data.

Secure execution of cryptographic algorithms (co-PI) **11/2015 – 12/2018**
- Grant: Intel/FAPESP Research Partnership for Technological Innovation, US$ 160,000.
- Objective: Design instruction set extensions for side-channel resistant cryptography.

University of Brasília, Brasília, Brazil

Physical Unclonable Functions for SoC Devices (co-PI) **07/2012 – 11/2015**
- Grant: Partnership with Intel Labs, US$ 87,000.
- Objective: Design energy-efficient constructions and protocols for PUF-based cryptography.

Selected Invited and Contributed Talks

"**A decade probing the Brazilian voting machine**". In IT Security Day, Germany, 2024.

"**Efficient software implementation of curve-based cryptography**". In Summer School on Real-world Crypto and Privacy, Croatia, 2022.

"**Security and privacy challenges in modern embedded systems**". In *Grundfos Archimedes Lecture*, Denmark, 2019.

"**Return of the insecure Brazilian voting machines**". In *DEF CON Voting Village*, USA, 2018; *Black Hat Asia*, Singapore, 2019; *Workshop on E-lections*, Israel, 2019; InfoSecurity Denmark, 2019.

"**Pairings are not dead, just resting**", "**Introduction to pairings**". In *21st Workshop on Elliptic Curve Cryptography (ECC)*, Netherlands, 2017.

"**Lightweight cryptography on ARM**". In *Software Performance Enhancement of Encryption and Decryption and Benchmarking (SPEED-B)*, Netherlands, 2016; and *NIST Lightweight Cryptography Workshop (LWC)*, USA, 2016.

"**Software vulnerabilities in the Brazilian voting machine**". In *5th Real World Cryptography Conference (RWC)*, USA, 2016.

"**Security Analysis of the Brazilian voting machine**", "**Software implementation of pairings**". In *3rd Advanced School on Cryptology and Information Security in Latin America (AS-Crypto)*, Mexico, 2015.

"**Efficient binary field arithmetic and applications to curve-based cryptography**". In *14th International Workshop on Cryptographic Hardware and Embedded Systems (CHES)*, Belgium, 2012; and Microsoft Research (MSR), USA, 2012.

"**Software vulnerabilities in the Brazilian voting machine**". In *Electronic Voting Technology/Workshop on Trustworthy Elections (USENIX EVT/WOTE)*, USA, 2012.

"**Software implementation of pairings**". In *The 15th Workshop on Elliptic Curve Cryptography (ECC)*, France, 2011.

"**High-speed parallel software implementation of the η_T pairing**". In *Software Performance Enhancement of Encryption and Decryption and Cryptographic Compilers (SPEED-CC)*, Germany, 2009.

Professional Service

Co-Editor in Chief of IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES) and **Program co-Chair** of CHES 2023.

Program co-Chair of LATINCRYPT 2014 and SBSEG 2014 (Brazilian Symposium on Information and Computational Systems Security).

Co-founder and Program Co-Chair for two editions of the Workshop on Election Technology (WTE), the first academic workshop in Brazil for research on this topic.

Steering Committee member of the LATINCRYPT and CHES conferences.

Editoral Board member of Journal of Universal Computer Science (JUCS).

Program Committee member of top conferences in Computer Security and Cryptography, including CRYPTO 2025, EUROCRYPT 2024/2025, USENIX Security 2024, CHES 2017-2019/2021-2022/2025, SAC 2018-2021, FC 2017-2021, PKC 2018-2019, LATINCRYPT 2015/2017/2019/2023, INDOCRYPT 2016/2018/2019.

Reviewer for over 40 academic journals, including Journal of Cryptographic Engineering, IEEE Transactions on Computers, IEEE Security and Privacy, IEEE Transactions on Circuits and Systems, IEEE Transactions on Dependable and Secure Computing, IEEE Transactions on Information Forensics and Security, IEEE Transactions on VLSI, IEEE Transactions on Information Theory, ACM Transactions on Embedded Computing Systems, The Computer Journal, Designs, Codes and Cryptography, Journal of Cryptology.

Reviewer for grant proposals submitted to Ministry of Science, Technology and Space in Israel; the São Paulo Research Support Foundation (FAPESP) in Brazil; and Comisión Nacional de Investigación Científica y Tecnológica (CONACYCT/ANID) in Chile, European Research Council (ERC).

Membership

Principal Investigator at the Concordium Blockchain Research Center. Work Package Leader in Cybersecurity at the DIGIT Centre for Digitalisation, Big Data and Data Analytics.

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

Community Outreach

Challenge designer and online instructor for the Cryptography track in the local, regional and national Capture-The-Flag (CTF) competitions that qualify teams for the European Cybersecurity Challenge.

International Relations

Long-term collaborations with groups at University of Campinas (Brazil), Technology Innovation Institute (UAE), NTT Secure Platform Laboratories (Japan), NTNU (Norway). My research has been featured in more than 150 news pieces in Brazil and international press, including La Nación, Ars Technica, Spiegel Online, The Economist, ZDNet, New York Times.

Software

Lead developer and founder of the RELIC cryptographic toolkit: `http://github.com/relic-toolkit`