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://sites.google.com/site/dfaranha

Research Objectives

Enable the development of a new generation 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 for banking infrastructure and electronic voting.

Public Profiles

- 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 undergrad courses on Computer Architecture and grad courses on Systems Security.

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

University of Campinas, Campinas, Brazil
Assistant Professor, Institute of Computing **02/2014 – 06/2018**
- Researcher on Cryptographic Engineering and Systems Security.
- Lectured undergrad courses 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 undergrad 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 encrypted messaging in C++ and JavaScript employing pairing-based cryptography.

Honors and Awards

- Supervisor of Best MSc. Dissertation defended in Brazil on Computer Architecture and High-Performance Computing **2019**
- Top 1% reviewers for cross-field research on Publons **2018**
- Invited to discuss security issues with electronic voting at Brazilian Senate **2018**
- Selected to defend 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, awarded by MIT TechReview for work in electronic voting **2015**
- Raised US$ 30,000 in crowdfunding campaign for YouInspect project **2014**
- Best Paper Award in CHES **2013**
- Best PhD dissertation in Brazil on Computer Security and Cryptography **2012**
- 2nd Best Computer Science PhD Thesis in Brazil, awarded 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

Completed supervisions: 29 undergrad research and final projects, 5 MSc. dissertations, 4 MSc. co-supervisions, 2 PhD co-supervisions, 1 Postdoc.

Publications: 22 journal articles, 3 book chapters, 37 papers in conference proceedings, 7 papers in peer-reviewed workshops.

Citations: 2199 (Google Scholar), 1089 (ResearchGate), 777 (Scopus), 472 (ISI).

H-Index: 23 (Google Scholar), 18 (ResearchGate), 15 (Scopus), 15 (ISI).

Funding

Aarhus University, Aarhus, Denmark

RENAIS: Residue Number Systems for Cryptography (PI) **07/2021 – Present**

- Grant: Independent Research Fund Denmark, DKK 2,871,000
- Objective: Develop algorithms for field arithmetic in RNS representation.

BAN – Blockchain Network Academy (PI) **01/2020 – Present**

- 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.

Verifiable cryptographic software (PI) **08/2019 – Present**

- Grant: Partnership with Concordium Blockchain Research Center, DKK 2,250,000.
- Objective: Develop techniques for formal verification of cryptographic software.

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

"**Return of the insecure Brazilian voting machines**". In *DEF CON 26 Voting Village*, USA, 2018; *Black Hat Asia*, Singapore, 2019; *Workshop on E-lections*, Israel, 2019; InfoSecurity Denmark, 2019.

"**Security and privacy challenges in modern embedded systems**". In *Grundfos Archimedes Lecture*, 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)*, Stanford, 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/Workshop on Trustworthy Elections (USENIX EVT/WOTE)*, USA, 2012.

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

PhD. and Postdoc Supervisions

Benjamin Salling Hvaas, PhD student at Aarhus University (co-supervision)
Topic: *Verifiable pairing-based cryptographic software* **08/2019 – Present**

Akira Takahashi, PhD student at Aarhus University (co-supervision)
Topic: *Fault side-channel attacks on signature schemes* **01/2019 – Present**

Antônio Carlos Guimarães Junior, PhD student at University of Campinas (co-supervision)
Topic: *Privacy-preserving computation in the cloud* **07/2019 – Present**

Rogério Vinicius Matos Rocha, PhD student at University of Campinas
Topic: *Differential Privacy in automotive applications* **03/2017 – Present**

Pedro Geraldo Morelli Rodrigues Alves, PhD student at University of Campinas
Topic: *GPU-accelerated homomorphic encryption* **03/2016 – Present**

Jheyne Nayara Ortiz, PhD student at University of Campinas (co-supervision)
Topic: *Efficient parameters for lattice-based cryptography* **03/2016 – Present**

Amanda Cristina Davi Resende, PhD student at University of Campinas
Topic: *Private Set Intersection protocols* **03/2015 – Present**

Narcise B. Mbiang, PhD student at University of Dschang, Cameroon (co-supervision)
Topic: *Computing the Optimal Ate pairing at high security levels* **03/2015 – Present**

Caio Hoffman, PhD at University of Campinas (co-supervision)
Topic: *Computer Security by Hardware-Intrinsic Authentication* **09/2015 – 01/2019**

Eduardo Moraes de Morais, PhD at University of Campinas (co-supervision)
Topic: *CCA1-Secure Somewhat Homomorphic Encryption* **04/2010 – 06/2016**

Karina Mochetti de Magalhães, Postdoc at University of Campinas
Topic: *Formal security analysis of PUF-based protocols* **04/2015 – 11/2015**

MSc. Supervisions

Joseph Alnajjar, MSc at Aarhus University (co-supervision)
Topic: *Efficient implementation of new families of pairing-friendly curves* **01/2019 – 07/2019**

Antônio Carlos Guimarães Junior, MSc at University of Campinas
Topic: *Secure and efficient implementation of code-based cryptography* **03/2017 – 01/2019**

Otávio Oliveira Napoli, MSc at University of Campinas (co-supervision)
Topic: *Timing Side-Channel Analysis of Dynamic Binary Translators* **03/2017 – 04/2019**

Hayato Fujii, MSc at University of Campinas
Topic: *Efficient Curve25519 Implementation for ARM Microcontrollers* **03/2016 – 05/2018**

Edson Floriano de Sousa Junior, MSc at University of Brasília (co-supervision)
Topic: *Privacy in Shared-memory Tuple Spaces* **03/2015 – 12/2017**

Jheyne Nayara Ortiz, MSc at University of Campinas (co-supervision)
Topic: *Efficient secure Gaussian sampling for lattice-based cryptography* **03/2014 – 03/2016**

Hilder Vitor Lima Pereira, MSc at University of Campinas
Topic: *Machine learning over encrypted data* **07/2014 – 09/2016**

Pedro Geraldo Morelli Rodrigues Alves, MSc at University of Campinas
Topic: *Computing over encrypted data using GPGPUs* **07/2014 – 07/2016**

Amanda Cristina Davi Resende, MSc at University of Brasília
Topic: *PUF-based cryptographic protocols* **02/2013 – 02/2015**

Workshop Presentations

"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.

"Efficient implementation of elliptic curves on sensor nodes", and "NanoPBC: Implementing Cryptographic Pairings on an 8-bit Platform". In *Conference on Hyperelliptic curves, discrete Logarithms, Encryption, etc.*, Chile, 2009.

Professional Service

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 conference.

Program Committee member of SBSEG 2012-2017, PAIRING 2013, ICFCNA 2014, ISC 2016, ACNS 2017, WAIFI 2018/2020, LightSec 2018, KANGACRYPT 2018, IEEE CCNC 2017-2019, LATINCRYPT 2015/2017/2019, INDOCRYPT 2016/2018/2019, FC 2017-2020, CHES 2017-2019, PKC 2018-2019, SAC 2018-2019, IEEE Wireless Africa 2019.

Editoral Board member of IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES), Journal of Universal Computer Science (JUCS) and Cambridge Experimental Results (ER).

Reviewer for 46 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 VLSI, IEEE Transactions on Information Theory, ACM Transactions on Embedded Computing Systems, The Computer Journal, Designs, Codes and Cryptography, Journal of Cryptology; and 31 academic conferences, including PKC, CT-RSA, ASIACRYPT and CHES.

Reviewer for grant proposals submitted to the Israeli 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) in Chile.

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

Co-founder and leader of YouInspect project (*Projeto Você Fiscal*) for voting machine (in)security awareness, election observation and crowdsourced verification of election results.

Software

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

Teaching Experience

Teaching experience described in detail by the portfolio table presented below.

Year	Title of course	Role	Type	Participants	Involvement	Level	Exam
2012	CIC 114785 – Object-Oriented Programming	Lecturer	60-hour classrom instruction	5 undergrads	Took over second half from a colleague	BSc., 3rd semester	2 written exams, 1 large programming project
2012	CIC 117366 – Computational Logic	Lecturer	60-hour classrom instruction	35 undergrads	Took over ongoing course	BSc., 2nd semester	2 written exams
2012	CIC 116785 – Architecture of Digital Processors	Lecturer	60-hour classrom instruction	Approx. 15 per term	Planning and conducting teaching.	BSc., 4th semester	2 written exams, seminar on advanced topic
2013	CIC 115432 – System Software	Lecturer	60-hour classrom instruction	19 in first term, 35 in second term	Materials, planning and conducting.	BSc., 6th semester	2 written exams, 3 programming projects
2012–2013	CIC 116947 – Competitive Programming	1/3 Lecturer	30-hour classrom, 30-hour lab	Approx. 15 per term	Restructuring, planning and conducting.	BSc., all levels	Programming contests
2012–2013	CIC 116458 – Theory of Encoding and Cryptography	Lecturer	60-hour classrom instruction	5 in first term, 13 in second	Restructuring, plannind and conducting.	BSc., last year	2 written exams, 3 programming projects
2012–2013	CIC 116475/116921 – Final Project I/II	Supervisor	Supervised BSc. final projects	5 projects, 6 students	Weekly meetings for feedback	BSc., last year	BSc. dissertation examination
2012	CIC 316504 – Topics in Computing (Cryptography)	Lecturer	60-hour classrom instruction	4 grad students	Creation, structuring, planning and teaching.	MSc., first year	2 written exams and 3 programming projects
2014–2016	MC030 – Undergraduate Final Project	Supervisor	Supervised advanced studies and final projects	6 students with individual projects	Weekly meetings for feedback, including examination	BSc., last year	BSc. dissertation examination
2014–2016	MC040/MC041 – Undergraduate Research Project I and II	Supervisor	Supervisor or undergrad research	6 students with individual projects	Weekly meetings for feedback, including examination	BSc., all levels	Manuscript examination
2014–2015	MC404 – Computer Organization and Assembly Programming	Lecturer	30-hour class, 30-hour lab instruction	Approx. 50 per term	Materials, planning, teaching.	BSc., 4th semester	2 written exams, 8 programming assignments
2015–2017	MC889/MO421 – Introduction to Cryptography	Lecturer	60-hour class instruction	Approx. 18 undergrads, 8 grad students per term	Materials, planning, teaching.	All levels	2 written exams, 3 programming projects
2015	MC931/MO834 – Secure Programming and Malware Analysis	1/2 Lecturer	60-hour class instruction	17 undergrad, 9 grad students	Materials, planning, teaching.	All levels	2 written exams, 5 programming assignments
2015–2016	MC102 – Algorithms and Computer Programming	Lecturer	60-hour class, 30-hour lab instruction	Approx. 50 per term	Conducting a coordinated course.	BSc., 2nd semester	2 written exams, 10 programming tasks
2016	MC621/MC821 – Competitive Programming Challenges	1/2 Lecturer	15-hour class, 45-hour lab	Approx. 15 per term	Lecturing classes.	BSc., senior	Programming contests
2016–2017	MC721/MC921 – Competitive Programming Challenges II	1/2 Lecturer	15-hour class, 45-hour lab	Approx. 15 per term	Lecturing classes.	BSc., senior	Programming contests
2014	MO417 – Algorithm Complexity	Lecturer	60-hour class instruction	27 grad students	Materials, planning, teaching.	MSc./PhD., first year	3 written exams and 7 problem sets
2019	Internet of Things Technology	Examiner	60-hour class instruction	17 grad students	Internal co-examiner	MSc.	Oral examination
2019	Fundamentals of Computer Security	Lecturer	60-hour class instruction	4 grad students	Materials, planning, teaching.	MSc., second year	3 practical assignments and 1 final report
2020	Algorithms and Data Structures	Lecturer	60-hour class instruction	25 undergrad students	Materials, planning, teaching.	BSc., second year	7 Hand-ins and 1 written exam
2020	Network Security	Lecturer	60-hour class instruction	50 grad students	Materials, planning, teaching.	MSc., senior	3 programming assignments and 1 final project
2021	Computer Architecture, Operating Systems and Networks	Lecturer	60-hour class instruction	100 undergrad students	Teaching half of the course	BSc., senior	10 hand-ins and 1 written exam