Pedro G. M. R. Alves

Contact Information

Address: Campinas, São Paulo, Brazil
Email: pdroalves@gmail.com | pedro.alves@zama.org
Website: www.iampedro.com
Profiles: GitHub | LinkedIn | ORCID | Google Scholar

Research Interests

- Applied cryptography,
- Cryptographic engineering,
- Privacy-preserving computing,
- Secure communication,
- High performance computing,
- GPGPUs,
- Zero-knowledge proofs.

Professional Experience

2022 – At present | Senior GPU Engineer
Zama, Paris - France.
Development of a CUDA-based library to offer the arithmetic needed to accelerate TFHE.
Responsible for the creation and maintenance of `zk-cuda-backend`, a CUDA-accelerated backend for zero-knowledge proof generation within the TFHE-rs ecosystem.

2013 – 2014 | Business Intelligence Analyst.
Kanui, São Paulo - SP - Brazil.
Development of automation systems with intense manipulation of databases, data extraction and processing. Responsible for the IT team in auditing of two Rocket Internet ventures.

2013 | Software Development Intern.
Kanui, São Paulo - SP - Brazil.
Development of automation systems with intense manipulation of databases, data extraction and processing using mainly Python.

Education

2016 – 2023 | PhD in Computer Science, **University of Campinas**, Campinas - SP - Brazil.
Thesis: "Cryptographic engineering of privacy-preserving algorithms".
Advisor: Prof. Diego F. Aranha.

2014 – 2016 | MSc in Computer Science, **University of Campinas**, Campinas - SP - Brazil.
Dissertation: "Efficient GPGPU implementation of the Leveled Fully Homomorphic Encryption scheme YASHE".
Advisor: Prof. Diego F. Aranha.

2008 – 2013 | Bachelor of Applied and Computational Mathematics, **University of Campinas**, Campinas - SP - Brazil.

Academic Experience

2020 – 2021 | Visiting doctoral researcher.
University of Aarhus, Aarhus - Denmark.
Advisor: Prof. Diego F. Aranha.
The focus is on the development of strategies for efficient implementation and applicability of different solutions for privacy-preserving data management and computing. As starting points, we shall continue previous efforts on the acceleration of functional encryption schemes (such as homomorphic encryption) using GPGPU-parallelism and applying it on real-world applications, such as human face recognition, an otherwise notoriously privacy-intrusive computing task.

I Sem. 2017 | Teaching assistant – Algorithms and Computer Programming – MC102.
Institute of Computing, University of Campinas, Campinas - SP.
Professor: Guido Araujo.
Syllabus: First contact with computer programming. Algorithms, systematic development, debugging, testing and documentation of programs.

II Sem. 2016 | Teaching assistant – Algorithms and Computer Programming – MC102.
Institute of Computing, University of Campinas, Campinas - SP.
Professor: Diego F. Aranha.
Syllabus: First contact with computer programming. Algorithms, systematic development, debugging, testing and documentation of programs.

I Sem. 2015 | Teaching assistant – Object Oriented Programming – MC302.
Institute of Computing, University of Campinas, Campinas - SP.
Professor: André Santanchè.
Syllabus: Basics and advanced concepts of object-oriented programming. Application of concepts through Java language.

II Sem. 2014 | Teaching assistant – Programming Paradigms – MC346.
Institute of Computing, University of Campinas, Campinas - SP.
Professor: João Meidanis.
Syllabus: Comparative overview of programming paradigms. Functional, logic and object-oriented programming.

2012 – 2013 | Research in Scientific Initiation Program.
Brazilian Biosciences National Laboratory, Campinas - SP - Brazil.
Advisor: PhD. Marcio Chaim Bajgelman.
Software development in C and Java for analysis of huge cDNA libraries with high performance using the CUDA platform.

2010 – 2011 | Research in Scientific Initiation Program.
Institute of Mathematics, Statistics and Scientific Computing, University of Campinas, Campinas - SP - Brazil.
Advisor: Prof. Ricardo Biloti.
Study of the implementation of numerical methods for geophysics simulations using parallel algorithms and CUDA.

Publications

2024, TCJ | **Alves, P. G. M. R.** et al.
"*Lattice-Based Homomorphic Encryption For Privacy-Preserving Smart Meter Data Analytics*"
In *The Computer Journal*.

2021, FC | **Alves, P. G. M. R.**, Ortiz, J.N, and Aranha, D. F.
"*Faster Homomorphic Encryption over GPGPUs via hierarchical DGT*"
In *Financial Cryptography and Data Security*.

2018, JISA | **Alves, P. G. M. R.** and Aranha, D. F.
"*A framework for searching encrypted databases*".
In *Journal of Internet Services and Applications*, 9(1), 1.

2016, SBSeg | **Alves, P. G. M. R.** and Aranha, D. F.
"*A framework for searching encrypted databases*" – **Best paper runner-up**.
In *XVI Brazilian Symposium on Information and Computational Systems Security*, Niterói - RJ - Brazil.

2016, CTDSeg | **Alves, P. G. M. R.** and Aranha, D. F.
"*Efficient GPGPU implementation of the Leveled Fully Homomorphic Encryption scheme YASHE*" (In Portuguese) – **Finalist**.
In *IV Contest of Theses and Dissertations on Information and Computational Systems Security*, Niterói - RJ - Brazil.

2016, CSBC | **Alves, P. G. M. R.** and Aranha, D. F.
"*Efficient GPGPU implementation of the Leveled Fully Homomorphic Encryption scheme YASHE*" (In Portuguese).
In *Congress of the Brazilian Computer Society*, Porto Alegre - RS - Brazil.

2015, SBSeg | **Alves, P. G. M. R.** and Aranha, D. F.
"*cuYASHE: Computation over encrypted data on GPGPUs*" (In Portuguese).
In *XV Brazilian Symposium on Information and Computational Systems Security*, Florianópolis - SC - Brazil.

2011, CISBGf | **Alves, P. G. M. R.** and Biloti, R.
"*Ray tracing in GPGPUs*" (In Portuguese).
In *12th International Congress of the Brazilian Geophysical Society*, Rio de Janeiro - RJ - Brazil.

Relevant programming projects

2025 – At present	**Farewell – Decentralized Posthumous Messaging.** Personal project. A decentralized application using smart contracts on FHEVM for posthumous encrypted messaging with check-in mechanisms and grace periods. Deployed on Ethereum Sepolia testnet.
2022 – At present	**TFHE-rs – Pure Rust Implementation of TFHE.** Zama. Contributor to Zama's open-source pure Rust implementation of TFHE for encrypted boolean and integer arithmetic, implementing programmable bootstrapping and advanced FHE features. https://github.com/zama-ai/tfhe-rs
2017 – 2023	**SPOG and cuPoly – Secure Processing on GPGPUs.** University of Campinas. SPOG is a continuation of the work with cuYASHE that explores different homomorphic cryptosystems on a modular design, allowing easy code reuse on different schemes. SPOG was first presented on FC21 and today implements two homomorphic cryptosystems, BFV and CKKS, with considerable speed-ups for both. https://github.com/spog-library
2014 – 2016	**cuYASHE.** University of Campinas. cuYASHE was the first implementation of the homomorphic scheme YASHE on GPGPUs. This library employs the CUDA platform and some algebraic techniques (like CRT, FFT and optimizations on polynomial and modular reduction) to obtain significant performance improvements. https://github.com/cuyashe-library

Personal Data

Citizenship	Brazilian
Date of Birth	August 27, 1988

Language Skills

Portuguese	Native language.
English	Fluent.

Technical Skills

Operational Systems:	GNU/Linux, Mac OS and Windows.
Languages:	**Rust**, **C/C++**, **Python**, Solidity, Java, JavaScript, Bash Script, Prolog, Lisp.
Information Security:	Expert in **cryptography** with **practical and theoretical knowledge** of the efficient implementation of cryptographic algorithms and **deep knowledge** of current **functional encryption** schemes and **differential privacy** methods.
Databases:	**SQL**: MySQL, MariaDB, SQLite, PostgreSQL. **NoSQL**: MongoDB, Redis and others.
Parallelism:	**CUDA**, **PThreads**, **OpenMP**, **MPI** and **MapReduce** techniques.
Internet Frameworks:	**Django**, **Node.JS** and **Socket.IO**.
Cloud Computing:	**Google Cloud**, **AWS**, **Hyperstack** and others.
Software Engineering:	Experience with **Scrum** and **UML**.
Versioning:	**Git**.