

Pedro G. M. R. ALVES

CONTACT INFORMATION

ADDRESS: Campinas, São Paulo, Brazil

EMAIL: pdroalves@gmail.com

WEBSITE: www.iampedro.com

RESEARCH INTERESTS

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

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 (as homomorphic encryption) using GPGPU-parallelism and applying it on real-world applications, as human face recognition an otherwise notoriously privacy-intrusive computing tasks.
- 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 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.

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.

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 TI 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.

CONFERENCE PUBLICATIONS

- 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 Society of Geophysical*, Rio de Janeiro - RJ - Brazil.

RELEVANT PROGRAMMING PROJECTS

- 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 technics (like CRT, FFT and optimizations on polynomial and modular reduction) to obtain significant performance improvements.
<https://github.com/cuyashe-library>

EDUCATION

2016 – 2023	PhD in COMPUTER SCIENCE, University of Campinas , Campinas - SP - Brazil. Advisor: Prof. Diego F. ARANHA.
2014 – 2016	MSc in COMPUTER SCIENCE, University of Campinas , Campinas - SP - Brazil. <i>Dissertation</i> : “Computation over encrypted data on GPGPUs”. Advisor: Prof. Diego F. ARANHA.
2008 – 2013	Bachelor of APPLIED AND COMPUTATIONAL MATHEMATICS, University of Campinas , Campinas - SP - Brazil.

PERSONAL DATA

CITIZENSHIP	Brazilian
DATE OF BIRTH	August 27, 1988

LANGUAGE SKILLS

PORTUGUESE	Mother language.
ENGLISH	Fluent.

TECHNICAL SKILLS

Operational Systems:	GNU/LINUX, MAC OS and WINDOWS.
Languages:	C, Python, 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, Oracle. NoSQL : MongoDB, Redis, Berkeley DB, HamsterDB and Neo4j.
Parallelism:	CUDA, PThreads, OpenMP, MPI and MapReduce techniques.
Internet Frameworks:	Django, Node.JS and Socket.IO .
Cloud Computing:	Google Cloud and AWS .
Software Engineering:	Experience with Scrum and UML .
Versioning:	Git and Mercury .