Pedro G. M. R. Alves

Contact Information

Address: Institute of Computing, University of Campinas.
Av. Albert Einstein, 1251 - CEP 13083-852, Campinas/SP - Brazil
Email: pedro.alves@ic.unicamp.br
Website: www.iampedro.com

Research Interests

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

Academic Experience

2020 – At present

Visiting doctoral researcher.
University of Aarhus, Aarhus - Denmark.
Advisors: Prof. Daniel Lucani and 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

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.

Education

2016 – At present	PhD student 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. *Dissertation*: “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

Personal Interests

- Amateur runner training for his first marathon.
- Produce and present a podcast about popular culture and adult life.
- Photography enthusiast.

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**.