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

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

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

Language Skills

PORTUGUESE	Mother language.
ENGLISH	Fluent.

Technical Skills

Operational Systems:	GNU/LINUX, MAC OS and WINDOWS.
Languages:	**C**, **Java**, **Python**, **JavaScript**, **Shell Script**, **HTML5**, **CSS**, **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.
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 App Engine** and **AWS**.
Software Engineering:	Experience with **Scrum** and **UML**.
Versioning:	**Git** and **Mercury**.
Mobile:	Advanced knowledge in **Android** development using native code and HTML5, mainly **Sencha Touch**.