Vitor Manuel Parreira Pereira

https://vm2p.github.io vitorm2p@gmail.com
https://gitlab.com/vm2p https://github.com/vm2p

EDUCATION

MAP-i Doctoral Program — **Braga, Aveiro and Porto, Portugal**
PhD in Computer Science — *April 2020*

Universidade do Minho — **Braga, Portugal**
Master in Computer Science — *September 2015*

Universidade da Beira Interior — **Covilhã, Portugal**
Bachelor in Computer Science — *July 2013*

RESEARCH EXPERIENCE

Advanced Computer Scientist — **Menlo Park, CA, United States**
SRI International — *February 2021 - Ongoing*
Conducting research in the intersection of theoretical cryptography and formal methods, particularly research based on computer-aided cryptography, with focus on the development of machine-checked implementations of cryptographic software via code synthesis from mechanically verified cryptographic proofs in EasyCrypt. Also, participating in various government-funded projects, as well as participating in different proposal efforts.

Researcher — **Porto, Portugal**
HASLab – INESC TEC & DCC FC Universidade do Porto — *June 2020 - February 2021*
Responsible for a collaboration project between INESC TEC and SRI International with the goal of formally verify a zero-knowledge proof protocol based on the MPC-in-the-Head (MitH) construction. This project was carried out under the Securing Information for Encrypted Verification and Evaluation (SIEVE) program funded by the Defense Advanced Research Projects Agency (DARPA).

Researcher — **Porto, Portugal**
HASLab – INESC TEC & DCC FC Universidade do Porto — *July 2016 - April 2020*
Developed his Ph.D. thesis "Integrated verification of cryptographic security proofs and implementations", focusing on reducing the abstraction gap between cryptographic security proofs and real implementations.

Intern — **Menlo Park, CA, United States**
SRI International — *September 2018 - December 2018*
The goal of this internship was the study and development of Multiparty Computation (MPC) techniques that could be applied to the particular case of Blockchain usage, and to provide formal proofs/implementation of the techniques explored.

Particularly, the work focused on the use of EasyCrypt to deliver formal proofs of proactive secret sharing and MPC primitives, as well developing a new EasyCrypt extraction tool that could be used to generate a verified implementations of such primitives.

Intern — **Madrid, Spain**
Instituto IMDEA Software — *March 2016 - July 2016*
Finished the development of a security proof and a verified implementation in OCaml of a concrete instantiation of Yao's Secure Function Evaluation protocol using EasyCrypt.

Researcher — **Braga, Portugal**

HASLab – INESC TEC & DI Universidade do Minho *January 2015 - March 2016*
Developed his master thesis "*A deductive verification platform for cryptographic software*". The project consisted in developing a deductive verification platform for the CAO language, using the EasyCrypt toolset as a backend for the tool.

Started the development of a security proof and a verified implementation in OCaml of a concrete instantiation of Yao's Secure Function Evaluation protocol using EasyCrypt, in cooperation with the Cryptography team at IMDEA Software, Madrid.

Junior Researcher **Covilhã, Portugal**
RELiablE And SEcure Computation Group, UBI *January 2013 - July 2013*
Developed his undergraduate project "*Cloud Security: Homomorphic Encryption Schemes*", funded by Portugal Telecom - Inovação, under the PRICE (Privacy and Security Issues in Cloud Environment) project.

TEACHING EXPERIENCE

Assistant Lecturer **Porto, Portugal**
DCC FC Universidade do Porto *February 2019 - July 2019*
Assistant Lecturer of Functional Programming.

Functional Programming teaches students the funcional programming paradigm, using the Haskell language as support for the course activities.

Assistant Lecturer **Porto, Portugal**
DCC FC Universidade do Porto *April 2018 - July 2018*
Assistant Lecturer of Functional Programming.

Functional Programming teaches students the funcional programming paradigm, using the Haskell language as support for the course activities.

Assistant Monitor **Braga, Portugal**
Universidade do Minho *September 2015 - February 2016*
Assistant monitor at the Informatics Lab course.

Informatics Lab is an interdisciplinary course, where students practice what they learn in other courses, gaining also knowledge in useful mechanisms in Computer Science, such as the use of Unix shell or code documentation.

FUNDING

Principal Investigator *SRI International*
Internally funded

Principal Investigator of the 2022 project ALICE: Automated Late-stage Instrumentation of Cryptographic Executables, focused on the development of new tools and techniques for automatic patching of cryptographic software with verified implementations.

KEY SKILLS

Mother Tongue
Portuguese

Foreign Languages

	Understanding		Speaking		Writing
	Listening	Reading	Spoken Interaction	Spoken Production	
English	C2	C2	C2	C2	C1
Spanish	C2	C2	C1	C1	B1
French	B1	B1	B1	B1	B1

Digital Skills

- Software Formal Verification, including knowlege in COQ, Frama-C, Why3, F*, Model Checking and Abstract Interpretation
- Formal Verification of Cryptographic Primitives, including knowledge in EasyCrypt
- Analysis and Modeling of Software, including knowledge in Alloy
- Programmin in Functional Languages, such as OCaml, Haskell, F* or F#
- Compilers Development, using OCaml
- Cryptography

PUBLICATIONS

José Bacelar Almeida, Manuel Barbosa, Manuel L Correia, Karim Eldefrawy, Stéphane Graham-Lengrand, Hugo Pacheco and Vitor Pereira, *Machine-checked ZKP for NP-relations: Formally Verified Security Proofs and Implementations of MPC-in-the-Head*. ACM Conference on Computer and Communications Security (CCS) Seoul, South Korea 2021

Karim Eldefrawy and Vitor Pereira, *A High-Assurance Automatically Synthesized Evaluator for Machine-checked (Proactively) Secure Multi-party Computation Protocols*. ACM Conference on Computer and Communications Security (CCS) London, UK 2019

José Bacelar Almeida, Manuel Barbosa, Gilles Barthe, Matthew Campagna, Ernie Cohen, Benjamin Grégoire, Vitor Pereira, Bernardo Portela, Pierre-Yves Strub and Serdar Tasiran, *A Machine-Checked Proof of Security for AWS Key Management Service*. ACM Conference on Computer and Communications Security (CCS) London, UK 2019

José Bacelar Almeida, Manuel Barbosa, Gilles Barthe, Hugo Pacheco, Vitor Pereira, and Bernardo Portela, *Enforcing ideal-world leakage bounds in real-world secret sharing MPC frameworks*. In IEEE Computer Security Foundations Symposium (CSF), Oxford, UK, 2018

José Bacelar Almeida, Manuel Barbosa, Gilles Barthe, François Dupressoir, Benjamin Grégoire, Vincent Laporte and Vitor Pereira, *A Fast and Verified Software Stack for Secure Function Evaluation*. In ACM Conference on Computer and Communications Security (CCS), Dallas, TX, USA, 2017

Vitor Pereira, Simão Melo de Sousa, Paul Crocker and Ricardo Azevedo, *Criptografia Homomórfica como um Serviço: da Implementação à sua Aplicação*. In INForum, Évora, Portugal, 2013

AWARDS AND ACHIEVEMENTS

- Best Undergraduate Student of Computer Science in Beira Interior University, year 2013
- Won the Best Security Application developed in Beira Interior University, year 2013
- Won the Software Engineering course competition by developing the best application for a local enterprise
- Completed the course Crypto I, from Stanford University, with a final score of 100 per cent
- Received award for best student of Escola Secundária Quinta das Palmeiras - Covilhã for the academic year 2004/2005