Vitor Manuel Parreira Pereira

Curriculum Vitae

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*

WORK EXPERIENCE

Advanced Computer Scientist **Menlo Park, CA, United States**
SRI International *February 2021 - Ongoing*

My role at SRI involves participating in various US government-funded projects, as well as participating in different proposal efforts.

My research directions focus on 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.

Researcher **Porto, Portugal**
HASLab – INESC TEC & DCC FC Universidade do Porto *June 2020 - February 2021*

I was 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 my 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 my 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 my 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 functional 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 functional 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

Task Leader **ARPA-H funding**
SRI International *2023 to 2025*

Leader of the *Computer-Aided Cryptography for Health* (CAC-H) task, part of the *Cognitive Health Assistant that Learns and Organizes* (CHALO) project, part of the *Digital Health Security* (DIGIHEALS) ARPA-H program.

CAC-H focus on the development and deployment of the ALICE framework (listed bellow) to the concrete scenario of healthcare.

Principal Investigator **Internal Research and Development (IRAD) funding**
SRI International *2022 to 2024*

Principal Investigator of the *Instrumentation of Cryptographic Executables* (ALICE) project.

ALICE focus on the development of new tools and techniques for automatic patching of cryptographic code in binary executables with verified assembly implementations.

Co-Principal Investigator **DARPA funding**
SRI International *2021 to 2024*

Co-Principal Investigator of the *End-to-end Machinery for Proving Highly sensitive Application-oriented Statements In ZEro-knowledge* (EMPHASIZE) project, part of the *Securing Information for Encrypted Verification and Evaluation* (SIEVE) DARPA program.

EMPHASIZE focus on the development and deployment of machine-checked, formally verified implementations of zero-knowledge proof protocols, with particular emphasize on the efficiency of the final implementations.

PUBLICATIONS

1. Samuel Dittmer, Karim Eldefrawy, Stéphane Graham-Lengrand, Steve Lu, Rafail Ostrovsky and Vitor Pereira, *Boosting the Performance of High-Assurance Cryptography: Parallel Execution and Optimizing Memory Access in Formally-Verified Line-Point Zero-Knowledge*. ACM Conference on Computer and Communications Security (CCS) Copenhagen, Denmark 2023

2. 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

3. 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

4. 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

5. 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

6. 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

7. 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

SOFTWARE AND PROJECTS

EVOCrypt **EasyCrypt & OCaml**

https://github.com/SRI-CSL/zk-gen

EVOCrypt is a library that provides verified, high-assurance implementations of a series of cryptographic algorithms/protocols, including commitment schemes, MPC protocols, secret sharing schemes and ZK protocols.

All implementations have been first specified in EasyCrypt, where all security and functional correctness proofs have been formalized. OCaml code is then obtained via code synthesis using the CoCoCrypt toolchain. The properties proved in EasyCrypt are carried out to the final OCaml implementation, thus increasing the degree of assurance of our code.

ZKgen **OCaml**

https://github.com/SRI-CSL/zk-gen

ZKgen is a ZK platform that aggregates multiple ZK protocols into a single solution, giving the user the flexibility to chose which ZK protocol best fit its application scenario. It supports the evaluation of ZK relations written in SIEVE IR format.

ALICE **Python**

https://github.com/SRI-CSL/ALICE

The key features of ALICE are: i. automatically detecting and extracting implementations of weak or broken cryptographic primitives from binaries without requiring source code or debugging symbols; ii. identifying the context and scope in which such primitives are used, and performing program analysis to determine the effects of replacing such implementations with more secure ones; and iii. replacing implementations of weak primitives with those of stronger or more secure ones.

CoCoCrypt **OCaml**

https://github.com/SRI-CSL/cococrypt

EasyCrypt to OCaml extraction tool, focused on the functional core of EasyCrypt. It takes as input an EasyCrypt script and produces a WhyML file that matches the EasyCrypt file (and appropriate dependencies). Finally, it is possible to obtain verified OCaml code by relying on Why3 own extraction mechanism.

Patchkit **Ptyhon**

https://github.com/vm2p/patchkit

The Pathkit toolset, that patches an ELF binary using one or more simple Python scripts.

Machine-checked proof of security for AWS Key Management Service **EasyCrypt**

https://gitlab.com/kmsver/kmsdmp

EasyCrypt formalization of the AWS Key Management Service.

Machine-checked security proof of Yao's SFE protocol **EasyCrypt**

https://gitlab.com/gcircuits/yao

EasyCrypt formalization and corresponding verified implementation of the Yao's Secure Function Evaluation protocol.

KEY SKILLS

Languages

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

Digital Skills

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

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