FERNANDO VIRDIA

ISG, Royal Holloway, UoL | London, United Kingdom | f.virdia@gmx.com | https://fundamental.domains

Cryptographic researcher working on practical and theoretical aspects of post-quantum cryptography: construction and cryptanalysis of cryptographic schemes, mathematical optimisation for embedded devices, computational mathematics. Strong background in mathematics and information security, with technical experience with different programming languages and and operating systems.

WORK EXPERIENCE

May - Aug 2019 — **Cryptography research intern**
Microsoft Research, United States
- Security analysis of AES block cipher against quantum computers, using Q#
- Code-base and results made public at github.com/microsoft/grover-blocks

May - Aug 2018 — **Cryptography research intern**
Microsoft Research, United States
- C implementation of parallel collision finding for cryptanalysis of SIKE
- Code-base and results made public at github.com/microsoft/vOW4SIKE

Aug 2014 – Jul 2016 — **Front and back end developer**
Freelance, United Kingdom and Italy
- Web developer, plugin developer (Wordpress), custom back end refactoring
- Rewrote and expanded previous code-bases, adding interactivity and layout responsiveness

Mar 2015 – Sep 2015 — **JavaScript developer, system administrator**
Pro Gamma SpA, Italy
- Developed the mobile stack for the company's new JavaScript IDE
- Setup of the FreeBSD Gcloud servers used to host the new brand of services
- Used technologies: FreeBSD, JavaScript/NodeJs, Apache Cordova

PUBLICATIONS

A full list of scientific publications can be found on my personal website, or on Google Scholar.

EDUCATION

Sep 2016 – Mar 2021 (exp) — **PhD Information Security**
Royal Holloway, University of London, *United Kingdom*

Oct 2015 – Sep 2016 — **MSc Applied Mathematics, Distinction**
Imperial College London, United Kingdom

Oct 2011 – Aug 2014 — **BSc Mathematics, First Class Honours degree**
Imperial College London, United Kingdom

SKILLS

Languages — English proficient user, Italian and Spanish native speaker

IT
- Languages: JavaScript (including NodeJs and jQuery), C, Php, Python, SageMath, LaTeX proficient user
- Languages: Matlab, HTML5, CSS3, Sql, VB.Net, Maple, LaTeX basic user
- Operating systems: GNU/Linux, FreeBSD, Cygwin, Windows
- Software: GCC, Make, SSH, VirtualBox, WordPress, office suites, music editing and broadcasting software

Leadership and communication
- Chairman of the Linux Users' Group, year 2013-2014
- Coordinator of the students' society at school, moderator of school assemblies
- Member of the students' parliament of the Province of Milan

INTERESTS

- Rock climbing