Fernando Virdia

Applied Cryptography Group
Department of Computer Science
ETH Zurich
firstname.lastname@inf.ethz.ch
https://fundamental.domains

Current position

Post-doctoral researcher in Applied Cryptography
Applied Cryptography Group, ETH Zurich, Switzerland

My work focuses on practical and mathematical aspects of cryptanalysis and cryptography. My research centres on post-quantum security, with various works focusing on modelling concrete costs for cryptanalytic attacks. I am also interested in applications of cryptanalytic techniques to other fields.

Publications

2021 | On the Success Probability of Solving Unique SVP via BKZ
PKC 2021, eprint 2020/1308, code
E. W. Postlethwaite, F. Virdia
We refine predictions for the probability of solving Unique SVP when using BKZ or Progressive BKZ. We provide a heuristic analysis, extensive experiments, and an application to costing attacks against lattice-based cryptography.

2020 | Implementing Grover oracles for quantum key search on AES and LowMC
Eurocrypt 2020, eprint 2019/1146, code
S. Jaques, M. Naehrig, M. Roetteler, F. Virdia
We provide complete oracle designs for Grover key-search against AES and LowMC block ciphers, and provide overall circuit size estimations for attacks under depth restriction.

2020 | (One) failure is not an option: Bootstrapping the search for failures in lattice-based encryption schemes
Eurocrypt 2020, eprint 2019/1399, code
JP. D'Anvers, M. Rossi, F. Virdia
We provide a new attack strategy for accelerating failure search against non-perfect public key encryption and key encapsulation from lattices.

2020 | Improved Classical Cryptanalysis of SIKE in Practice
PKC 2020, eprint 2019/298, code
C. Costello, P Longa, M. Naehrig, J. Renes, F. Virdia
We investigate parallel collision finding for attacking SIKE and SIDH, finding small concrete speedups respect to previous work, both in general and via the algebraic structure of the particular problem.

2018 | Implementing RLWE-based Schemes Using an RSA Co-Processor
CHES 2019, eprint 2018/425, code
M. R. Albrecht, C. Hanser, A. Hoeller, T. Pöppelmann, F. Virdia, and A. Wallner
We repurpose existing RSA/ECC co-processors for (ideal) lattice-based cryptography by exploiting the availability of fast long integer multiplication.

2018 | Estimate All the {LWE, NTRU} Schemes!
SCN 2018, eprint 2018/331, website, code
M. R. Albrecht, B. R. Curtis, A. Deo, A. Davidson, R. Player, E. W. Postlethwaite, F. Virdia, and T. Wunderer
We investigate the impact that different estimates for the asymptotic runtime of (block-wise) lattice reduction have on the predicted security of LWE- and NTRU-based schemes submitted to NIST for standardisation.

2017 | Revisiting the expected cost of solving uSVP and applications to LWE
Asiacrypt 2017, eprint 2017/815, code
M. R. Albrecht, F. Göpfert, F. Virdia, and T. Wunderer
We compare success conditions proposed by Gama & Nguyen (Eurocrypt 2008) and by Alkim et al. (USENIX 2016) for solving the LWE problem by reducing it to the unique-SVP problem. We present empirical evidence in line with the latter estimate.

Education

2021 | PhD in Information Security
Royal Holloway, University of London, UK
Thesis: "Post-Quantum Cryptography: Cryptanalysis and Implementation", supervised by Martin R. Albrecht.

2016 | MSc in Applied Mathematics, Distinction
Imperial College London, UK
Thesis: "Geometry and spectrum of qutrit Hamiltonians", supervised by Ryan Barnett and Sania Jevtic.

2014 | BSc in Mathematics, First Class Honours
Imperial College London, UK
UROP research project on lattice-based hash functions.

Work Experience

2019 | Research intern
Microsoft Research, USA
Worked as part of the Security and Cryptography group on quantum cryptanalysis of block ciphers.

2018 | Research intern
Microsoft Research, USA
Worked as part of the Security and Cryptography group on cryptanalysis of isogeny-based key exchange.

2015 | Software developer
Progamma s.p.a., Italy
Developed the mobile stack for the company's new Javascript IDE, and worked on setting up the FreeBSD GCloud servers used to host the new brand of services.