Bernardo Magri

Curriculum Vitae

Oxford Rd.
Manchester, UK
✉ *bernardomagri21@gmail.com*
bernardomagri.eu
Nationality: Brazilian/Italian

"Anyone who attempts to generate random numbers by deterministic means is, of course, living in a state of sin."
–John von Neumann

Research Interests

My research interests are in all aspects of cryptography and security & privacy, including but not limited to foundations of blockchain technology, cryptographic protocols, subversion-resilient crypto, fuzzy cryptography and multiparty computation. I am also interested in computational complexity theory and distributed systems in general.

Formal Education

2017 **Ph.D. in Computer Science**, Sapienza University of Rome, Italy.

Advisor Giuseppe Ateniese.

Thesis title The Good, the Bad, and the (not so) Ugly: Many Facets of Cryptographic Backdoors.

2012 **M.Sc. in Computer Science**, University of São Paulo - IME, Brazil.

2008 **B.Sc. in Computer Science**, Universidade Paulista, Brazil.

Professional Experience

Dec 21–Present **Senior Lecturer (Associate Professor)**, The University of Manchester, UK.

Dec 18–Nov 21 **Post-doc Researcher**, Aarhus University, Denmark, Position funded by the Concordium Blockchain Research Center (COBRA).

Nov 16–Nov 18 **Post-doc Researcher *(Akademischer Rat)***, Friedrich-Alexander-Universität, Germany.

Mar 14–Nov 16 **Research Fellow**, Sapienza University of Rome, DIAG.

Publications

Conference Proceedings

(*) **The top 5 selected conference publications are marked with an asterisk**

[23] **Signature-based Witness Encryption with Compact Ciphertext** (with Gennaro Avitabile, Nico Döttling, Christos Sakkas and Stella Wohnig). AsiaCrypt 2024 (To appear)

[22] **Key Exchange in the Post-Snowden Era: Universally Composable Subversion-Resilient PAKE** (with Suvradip Chakraborty, Lorenzo Magliocco and Daniele Venturi). AsiaCrypt 2024 (To appear)

[21] **Certified Private Inference on Neural Networks via Lipschitz-Guided Abstraction Refinement** (with Edoardo Manino, Mustafa Mustafa and Lucas Cordeiro). Proceedings of the 6th Workshop on Formal Methods for ML-Enabled Autonomous Systems (FoMLAS@CAV 2023)

[20] **McFly: Verifiable Encryption to the Future Made Practical** (with Nico Döttling, Lucjan Hanzlik and Stella Wohnig). The 27th International Conference on Financial Cryptography and Data Security (FC 2023).

[19] **Revisiting Transaction Ledger Robustness in the Miner Extractable Value Era** (with Fredrik Kamphuis, Ricky Lamberty and Sebastian Faust). Proceedings of the 21st Applied Cryptography and Network Security (ACNS 2023).

[18] ***Universally Composable Subversion-Resilient Cryptography** (with Suvradip Chakraborty, Jesper Buus Nielsen and Daniele Venturi). 41st Annual International Conference on the Theory and Applications of Cryptology and Information Security (EuroCrypt'22).

[17] ***GearBox: Optimal-size Shard Committees by Leveraging the Safety-Liveness Dichotomy** (with Bernardo David, Christian Matt, Jesper Buus Nielsen and Daniel Tschudi). 29th ACM Conference on Computer and Communications Security (CCS'22).

[16] **Random-index PIR with Applications to Large-Scale Secure MPC** (with Craig Gentry, Shai Halevi, Jesper Buus Nielsen, and Sophia Yakoubov). The Theory of Cryptography Conference (TCC'21).

[15] **Weight-Based Nakamoto-Style Blockchains** (with Simon Holmgaard Kamp, Christian Matt, Jesper Buus Nielsen, Søren Eller Thomsen and Daniel Tschudi). 7th International Conference on Cryptology and Information Security in Latin America (LatinCrypt 2021).

[14] ***YOSO: You Only Speak Once / Secure MPC with Stateless Ephemeral Roles** (with Craig Gentry, Shai Halevi, Hugo Krawczyk, Jesper Buus Nielsen, Tal Rabin and Sophia Yakoubov). 41st Annual International Cryptology Conference (CRYPTO 2021).

[13] **Broadcast-Optimal Two Round MPC with an Honest Majority** (with Ivan Damgård, Luisa Siniscalchi and Sophia Yakoubov). 41st Annual International Cryptology Conference (CRYPTO 2021).

[12] ***Refresh When You Wake Up: Proactive Threshold Wallets with Offline Devices** (with Yashvanth Kondi, Claudio Orlandi and Omer Shlomovits). Proceedings of the 42nd IEEE Symposium on Security and Privacy (IEEE S&P 2021).

[11] **Reparo - A Publicly Verifiable Layer to Repair any Blockchain** (with Sri Aravinda Thyagarajan, Adithya Bhat, Daniel Tschudi and Aniket Kate). The 25th International Conference on Financial Cryptography and Data Security (FC 2021).

[10] **Afgjort - A Partially Synchronous Finality Layer for Blockchains** (with Thomas Dinsdale-Young, Christian Matt, Jesper Buus Nielsen and Daniel Tschudi). The 12th Conference on Security and Cryptography for Networks (SCN 2020).

[09] **Cryptographic Reverse Firewalls for Interactive Proof Systems** (with Chaya Ganesh and Daniele Venturi). The 47th International Colloquium on Automata, Languages and Programming (ICALP 2020).

[08] **Minting Mechanism for Proof of Stake Blockchains** (with Dominic Deuber, Nico Döttling, Giulio Malavolta and Sri Aravinda Thyagarajan). Proceedings of the 18th Applied Cryptography and Network Security (ACNS 2020).

[07] **Public Immunization Against Complete Subversion Without Random Oracles** (with Giuseppe Atenise, Danilo Francati and Daniele Venturi). Proceedings of the 17th Applied Cryptography and Network Security (ACNS 2019).

[06] **Redactable Blockchain in the Permissionless Setting** (with Dominic Deuber and S. A. Thyagarajan). Proceedings of the 40th IEEE Symposium on Security and Privacy (IEEE S&P 2019).

[05] **A Family of FDH Signature Schemes Based on the Quadratic Residuosity Assumption** (with Giuseppe Ateniese and Katharina Fech). Proceedings of the 19th International Conference on Cryptology in India (IndoCrypt 2018).

[04] **Secure Outsourcing of Cryptographic Circuits Manufacturing** (with Giuseppe Ateniese, Aggelos Kiayias, Yiannis Tselekounis and Daniele Venturi). Proceedings of the 12th International Conference on Provable Security (ProvSec 2018).

[03] ***Redactable Blockchain – or – Rewriting History in Bitcoin and Friends** (with Giuseppe Ateniese, Daniele Venturi and Ewerton Andrade). Proceedings of the 2nd IEEE Euro S&P Conference (IEEE Euro S&P 2017).

[02] **Subversion-Resilient Signature Schemes** (with Giuseppe Ateniese and Daniele Venturi). Proceedings of the 22nd ACM Conference on Computer and Communications Security (ACM CCS 2015).

[01] **Certified Bitcoins** (with Giuseppe Ateniese, Antonio Faonio and Breno de Medeiros). Proceedings of the 12th International Applied Cryptography and Network Security Conference (ACNS 2014).

Journals

[04] **Everlasting Composable Commitments from Fully Malicious PUFs** (with Giulio Malavolta, Dominique Schröder and Dominique Unruh). Journal of Cryptology, 2022.

[03] **Public Immunization Against Complete Subversion Without Random Oracles** (with Giuseppe Atenise, Danilo Francati and Daniele Venturi). Theoretical Computer Science, Elsevier. 2021.

[02] **Cryptographic Reverse Firewalls for Interactive Proof Systems** (with Chaya Ganesh and Daniele Venturi). Theoretical Computer Science, Elsevier. 2021.

[01] **Subversion-Resilient Signatures: Definitions, Constructions and Applications** (with Giuseppe Ateniese and Daniele Venturi). Theoretical Computer Science, Elsevier. 2020.

Patents Granted

2019 **Wrapped-Up Blockchain** US Patent No. 10356066

2019 **Hybrid Blockchain** US Patent No. 9959065, 10305875

2019 **Distributed Key Secret for Rewritable Blockchain** US Patent No. 9774578, 10110576

2018 **Rewritable Blockchain** US Patent No. 9967088, 9967096, 10243938, 10348707

2018 **Multiple-Link Blockchain** US Patent No. 9785369

Professional Activities

Program Committee '25 (EuroCrypt), '23 (CCS, ACNS), '22 (Crypto, ACNS, SECURWARE), '21 (ICSP, SECURWARE), 20' (ICSP, SECURWARE, Sicherheit), '19 (Provsec), '18 (ProvSec, Sicherheit)

Journal Reviewer Design Codes and Cryptography, ETRI Journal, Theoretical Computer Science, IEEE Transactions on Dependable and Secure Computing, IEEE Transactions on Information Forensics and Security.

Conf. External Reviewer TCC ('21, '24), ICDCS ('21), STOC ('20), CRYPTO ('19,'20, '23), PODC ('20), CCS ('15, '21), EuroCrypt ('16, '20), PKC ('16, '17, '18, '20), ESORICS ('16), AsiaCrypt ('16, '20), NDSS ('20), IWSec ('17), SacMat ('17), USENIX ('17), AsiaCCS ('17).

Recent Teaching Experience

Apr 23–May 23 *Lecturer* "Algorithms and Data Structures", The University of Manchester, UK

Sep 22–Oct 22 *Lecturer* "Cryptography", The University of Manchester, UK

Mar 22–Apr 22 *Lecturer* "Algorithms and Data Structures", The University of Manchester, UK

Mar 18–Apr 18 *Lecturer* for the intensive course "Cryptocurrencies", Friedrich-Alexander-Universität, Germany

Grants

2023-2026 **SECCOM: Securing composable hardware platforms** funded by DSTL (Defence Science & Technology Laboratory), Engineering & Physical Sciences Research Council (EPSRC). GBP 1,031,720 (or USD 1,313,271) in collaboration with Prof. John Goodacre and Prof. Lucas Cordeiro from the University of Manchester, UK (I am the Co-Investigator & WP leader).

Honors & Awards

Jun 16 **Best paper award in the computer science department**, for the paper "Subversion-Resilient Signature Schemes". *Sapienza University of Rome*, Italy.

Nov 12 **Best master's dissertation award at CTDSeg**, *Sociedade Brasileira de Computação*, Curitiba, Brazil.

Recent Talks

Jun 23 UK Crypto Day. London, UK.

Jun 23 Digital Trust and Security Guest Seminar Series. Manchester, UK.

Jun 22 Eurocrypt 2022. Trondheim, Norway.

Languages

Portuguese	Mothertongue
English	Fluent
Italian	Intermediate
German	Basic

Computer skills

Languages	C, C++, Pascal, Java, C#, Basic, Python, Bash script, LaTeX, Erlang, Lisp.
Frameworks	Qt, wxWidgets, .NET, JVM.
OS's	Unix/Linux, BSD, MacOS, Solaris.
Science	Maxima, Maple, Mathematica.
Softwares	Open/LibreOffice, Emacs.