Bernardo Magri

Curriculum Vitae

Åbogade, 34
Aarhus, Denmark
✉ *magri@cs.au.dk*
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, multiparty computation and etc. I'm 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 18–Present **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

[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). (to appear)

[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). (to appear)

[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).

(*) **The top 5 most relevant publications are marked with an asterisk**

Journals

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

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

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

Manuscripts

[07] **GearBox: An Efficient UC Sharded Ledger Leveraging the Safety-Liveness Dichotomy** (with Bernardo David, Christian Matt, Jesper Buus Nielsen and Daniel Tschudi).

[06] **Random-index PIR with Applications to Large-Scale Secure MPC** (with Craig Gentry, Shai Halevi, Jesper Buus Nielsen, and Sophia Yakoubov).

[05] **Broadcast-Optimal Two Round MPC with an Honest Majority** (with Ivan Damgård, Luisa Siniscalchi and Sophia Yakoubov).

[04] **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).

[03] **Everlasting Composable Commitments from Fully Malicious PUFs** (with Giulio Malavolta, Dominique Schröder and Dominique Unruh).

[02] **The Discriminating Miner Dilemma: Revisiting Liveness Guarantees under Content Preferences** (with Fredrik Kamphuis and Sebastian Faust).

[01] **A Framework for Weight-Based Nakamoto-Style Blockchains** (with Simon Holmgaard Kamp, Christian Matt, Jesper Buus Nielsen, Søren Eller Thomsen and Daniel Tschudi).

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 — ICSP '20, SECURWARE '20, ProvSec ('18, '19), SICHERHEIT ('18, '19)

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 — ICDCS ('21), STOC ('20), CRYPTO ('19,'20), PODC ('20), CCS ('15), EuroCrypt ('16, '20), PKC ('16, '17, '18, '20), ESORICS ('16), AsiaCrypt ('16, '20), NDSS ('20), IWSec ('17), SacMat ('17), USENIX ('17), AsiaCCS ('17).

Teaching Experience

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

Nov 17–Apr 18 — *Teaching Assistant* for the course "Cryptocurrencies", taught by Prof. Dominique Schröder, Friedrich-Alexander-Universität, Germany

Apr 17–Apr 17 *Teaching Assistant* for the intensive course "Cryptocurrencies", taught by Prof. Dominique Schröder, Friedrich-Alexander-Universität, Germany

Nov 16–Mar 17 *Teaching Assistant* for the course "Algorithmic Cryptography", taught by Prof. Dominique Schröder, Friedrich-Alexander-Universität, Germany

Jul 11–Jan 12 *Teaching Assistant* for the course "Segurança de Dados e Criptografia", taught by Prof. Routo Terada (in Portuguese), Universidade de São Paulo, Brazil

Grants

Feb 17 **COST Mission grant** to visit Prof. Dr. Daniele Venturi and his group for 7 days at Sapienza University of Rome, Italy.

Nov 16 **COST School grant** to attend COST-IACR School on Randomness in Cryptography, Barcelona, Spain.

May 16 **IACR grant** to attend the 2016 Eurocrypt conference, Vienna, Austria.

Oct 15 **ACM grant** to speak at the ACM CCS 2015 conference, Denver, USA.

Jun 14 **ACNS grant** to attend the ACNS 2014 conference, Lausanne, Switzerland.

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 Participation in Events

May 19 TPBC 2019. Aarhus, Denmark.

May 19 Eurocrypt 2019. Darmstadt, Germany

May 18 TPMPC 2018. Aarhus, Denmark.

May 17 Eurocrypt 2017. Paris, France.

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.