

# Bernardo Magri

## Curriculum Vitae

Fürther Straße 246c  
Nürnberg, Germany  
☎ +49 (911) 5302 96661  
✉ [bernardomagri21@gmail.com](mailto:bernardomagri21@gmail.com)  
🌐 [bernardomagri.com](http://bernardomagri.com)



*"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, including but not limited to, subversion attacks, signature schemes, blockchain technology, zero-knowledge proofs, verifiable computation, and etc. I'm also interested in computational complexity theory in general.

### Formal Education

- Nov 13–Feb 17 **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.  
Mar 08–Apr 12 **M.Sc. in Computer Science**, University of São Paulo - IME, Brazil.  
Feb 04–Feb 08 **B.Sc. in Computer Science**, Universidade Paulista, Brazil.

### Professional Experience

- Dec 18–Present **Post-doc Researcher**, Aarhus University, Denmark.  
Nov 16–Nov 18 **Post-doc Researcher (*Akademischer Rat*)**, Friedrich-Alexander-Universität, Germany.  
Mar 14–Nov 16 **Research Fellow**, Sapienza University of Rome, DIAG.  
Jul 11–Jan 12 **Teaching Assistant**, Universidade de São Paulo, IME.

### Publications

- [06] **Redactable Blockchain in the Permissionless Setting** (with Dominic Deuber and S. A. Thyagarajan), Proceedings of the 40th IEEE Symposium on Security and Privacy (S&P 2019), San Fransisco, CA, US, , pp. 645-659. doi:10.1109/SP.2019.00039
- [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), 364–375, ISBN 978-1-4503-3832-5.
- [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), 80–96, Lecture Notes in Computer Science 8479, ISBN 978-3-319-07535-8.

#### Manuscripts

- [04] **How to Immunize all Deterministic Primitives against Complete Subversion** (with Giuseppe Ateniese, Danilo Francati and Daniele Venturi).
- [03] **Minting Mechanisms for Blockchain – or – Moving From Crypto-Assets to Crypto-Currencies** (with Yulia Butkova, Dominic Deuber, Nico Döttling, Giulio Malavolta and Sri Aravinda Thyagarajan).
- [02] **Everlasting Composable Commitments from Malicious Hardware Assumptions** (with Giulio Malavolta, Dominique Schröder and Dominique Unruh).
- [01] **Subversion-Resilient Signatures: Definitions, Constructions and Applications** (with Giuseppe Ateniese and Daniele Venturi)

#### Patents

##### Granted

- 2018 US Patent No. 9967088, Rewritable Blockchain
- 2018 US Patent No. 9959065, Hybrid Blockchain
- 2018 US Patent No. 9785369, Multiple-Link Blockchain
- 2017 US Patent No. 9774578, Distributed Key Secret for Rewritable Blockchain

##### Pending

- US Publication No. 20180048469, Wrapped-Up Blockchain

#### 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.

#### 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.

## Professional Activities

- Program Committee ProvSec (2018), SICHERHEIT (2018)
- Journal Reviews ETRI Journal, Theoretical Computer Science (Elsevier), IEEE Transactions on Dependable and Secure Computing.
- External Reviewer ACM CCS (2015), Eurocrypt (2016), PKC (2016, 2017), ESORICS (2016), Asiacrypt (2016), IWSec (2017), SacMat (2017), USENIX (2017), AsiaCCS (2017).

## 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

## Participation in Events

- May 18 TPMPC 2018. Aarhus, Denmark.
- May 17 Eurocrypt. Paris, France.
- Nov 16 COST-IACR School on Randomness in Cryptography. Barcelona, Spain.
- May 16 IACR summer school on blockchains and cryptocurrencies. Corfu, Greece.
- May 16 Eurocrypt. Vienna, Austria.
- Oct 15 SPRITZ Workshop on Future Systems Security and Privacy. Padua, Italy. (*Speaker*)
- Oct 15 ACM CCS. Denver, USA. (*Speaker*)
- Jul 14 Summer school on black-box impossibility results. Bertinoro, Italy.
- Jun 14 ACNS. Lausanne, Switzerland.

## Languages

- Portuguese Mother tongue
- 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, Windows, MacOS, Solaris.
Science	Maxima, Maple, Mathematica.
Softwares	Open/LibreOffice, Emacs.

## Hobbies

Sports	(real) Football, MMA, Poker, Brazilian jiu-jitsu, Sailing.
Leisure	Traveling, Movies, TV series, Reading.

## References

The following people can attest for my professional qualifications.

### Giuseppe Ateniese

gatenies@stevens.edu ✉

The David and GG Farber endowed chair in Computer Science, Professor and Director  
Computer Science Department  
Stevens Institute of Technology, USA

### Daniele Venturi

venturi@di.uniroma1.it ✉

Assistant Professor  
Computer Science Department  
Sapienza University of Rome, Italy

### Nico Döttling

doettling@cispa.saarland ✉

Assistant Professor  
The CISPA – Helmholtz Center i.G., Germany