

Lorenzo Gentile

✉ lorg@itu.dk

🌐 <https://lorenzogentile404.github.io/>

🌐 <https://www.linkedin.com/in/lorenzogentile404/>

📺 <https://www.youtube.com/@lorenzogentile404>



Work Experience

- 11/2019 - 01/2023 **PhD Student at IT University of Copenhagen - Computer Science Department, Copenhagen - Denmark**
Thesis: *Expanding Blockchain Horizons through Privacy-Preserving Computation*
Advisor: Bernardo David (<https://www.bmdavid.com/>)
- Research focused on cryptographic protocols for multiparty computation and blockchain applications.
- Scientific Partner at Concordium, Copenhagen - Denmark**
Collaboration with Concordium on multiparty computation as part of IT University of Copenhagen cryptography's research group.
- 03/2022 - 08/2022 **Guest PhD Student at Technische Universität Darmstadt - Computer Science Department, Darmstadt - Germany**
Pursue my PhD research project in a new environment supported by a scholarship from Collaborative Research Center 1119 CROSSING.
- 10/2018 - 10/2019 **Research Assistant at IT University of Copenhagen - Business IT Department, Copenhagen - Denmark**
Contribution to the analysis and the design of blockchain based systems, implementation of solutions to conduct research activities and to the organization of educational activities.
- 01/2018 – 10/2019 **Freelance Software Engineer**
Contribution to numerous projects with a focus on statistical and simulation software.
- 04/2018 – 09/2018 **Technical Consultant at Observatory on Blockchain and Distributed Ledger - School of Management of Politecnico di Milano, Milan - Italy**
Contribution to a comparative analysis of the state-of-the-art blockchain projects and to the creation of educational contents.
- Research Collaborator at Politecnico di Milano - Dipartimento di Matematica, Milan - Italy**
Investigation related to the usage of blockchain in the insurance field.

- 09/2015 – 09/2017 ■ **Analyst and Developer at MOXOFF S.p.A. (spinoff Politecnico di Milano), Milan - Italy**
Research, design and development of mathematical, numerical and statistical methods for industrial application.
- 06/2008 ■ **Software Developer at Politecnico di Milano - Dipartimento di Elettrotecnica, Milan - Italy**
Development of a home automation software using Zigbee devices.

Education

- 11/2019 – 01/2023 ■ **Doctor of Philosophy - PhD, Computer Science at IT University of Copenhagen, Copenhagen - Denmark**
Thesis: *Expanding Blockchain Horizons through Privacy-Preserving Computation*
Advisor: Bernardo David (<https://www.bmdavid.com/>)

Research focused on cryptographic protocols for multiparty computation and blockchain applications.
- 09/2017 – 10/2017 ■ **Entrepreneurship at Draper University, San Mateo - California**
Program in Silicon Valley that offered essential startup skills, exposure to industry experts, a network of entrepreneurs and mentorship from experienced venture capitalists (<https://www.draperuniversity.com/>).
- 10/2012 – 07/2015 ■ **M.Sc. in Engineering of Computing Systems at Politecnico di Milano, Milan - Italy**
Thesis: *A comparative study of mechanisms for Sponsored Search Auctions* (https://www.politesi.polimi.it/bitstream/10589/108785/3/2015_07_Gentile_Gentile.pdf)
Advisor: Nicola Gatti (<http://www.gametheory.polimi.it/nicola-gatti.html>)

Studies focused on Mathematical Optimization, Mechanism Design and Machine Learning.
- 09/2009 – 09/2012 ■ **B.Sc. in Engineering of Computing Systems at Politecnico di Milano, Milan - Italy**
Final project: *a Java implementation of the Carcassonne board game*
- 09/2004 – 07/2009 ■ **Secondary School Diploma in Information Technology at Istituto di Istruzione Superiore Luigi Galvani, Milan - Italy**
Thesis: *Zigbee Technology and its Applications*

Research Publications

- 1 Brorsson, J., David, B., **Gentile, L.**, Pagnin, E., & Wagner, P. S. (2023). PAPR: Publicly Auditable Privacy Revocation for Anonymous Credentials. Cryptology ePrint Archive, Paper 2023/137. <https://eprint.iacr.org/2023/137> (published to CT-RSA 2023).

- 2 Baum, C., Chiang, J. H.-y., David, B., Frederiksen, T. K., & **Gentile, L.** (2021). SoK: Mitigation of Front-running in Decentralized Finance. Cryptology ePrint Archive, Report 2021/1628. <https://ia.cr/2021/1628> (published to DeFi 2022 - FC 2022 workshop).
- 3 David, B., **Gentile, L.**, & Pourpouneh, M. (2021). FAST: Fair Auctions via Secret Transactions. Cryptology ePrint Archive, Report 2021/264. <https://eprint.iacr.org/2021/264> (published to ACNS 2022).
- 4 Beck, R., Kubach, M., Jørgensen, K., Sellung, R., Schunck, C., & **Gentile, L.** (2019). *Study on the economic impact of blockchain on the danish industry and labor market*. <https://pure.itu.dk/da/publications/study-on-the-economic-impact-of-blockchain-on-the-danish-industry> (commissioned to IT University of Copenhagen).
- 5 Beck, R., Spasovski, J., **Gentile, L.**, & Mukkamala, A. M. (2019). *EmisChain - An application of blockchain technology for road-transport emissions monitoring to support an emissions market and an in-use emissions-based tolling system in the EU*. <https://www.ebcc.eu/wp-content/uploads/2023/02/EmisChain-230131.pdf> (commissioned to IT University of Copenhagen).
- 6 Bruschi, F., Rana, V., **Gentile, L.**, & Sciuto, D. (2019). Mine with it or sell it: the superhashing power dilemma. *SIGMETRICS Perform. Eval. Rev.* 46(3), 127–130. <https://dl.acm.org/doi/10.1145/3308897.3308954> (published to SOCCA 2018 - ACM SIGMETRICS Performance Evaluation Review symposium).

Selected Teaching and Dissemination Activities

- 06/2022 **20th International Conference on Applied Cryptography and Network Security (ACNS 2022), Rome - Italy**
 At ACNS, an annual conference focusing on current developments that advance the areas of applied cryptography and its application to systems and network security, I had the chance to present [3] (<https://acns22.di.uniroma1.it/>).
- 08/2021 - 01/2022 **Security 1 - IT University of Copenhagen, Copenhagen - Denmark**
 This is an introductory course on information security. The course focuses on introductory aspects of analysis, design and implementation of secure software.
- 01/2021 - 06/2021 **Cryptographic Computation and Blockchain - IT University of Copenhagen, Copenhagen - Denmark**
 This course introduces basic concepts and techniques for designing and analysing cryptographic protocols with a focus on privacy preserving computation and blockchain protocols. It covers both the main constructions of such protocols and the theoretical models used for proving their security.
- 08/2020 - 01/2021 **Security 1 - IT University of Copenhagen, Copenhagen - Denmark**
 This is an introductory course on information security. The course focuses on introductory aspects of analysis, design and implementation of secure software.

Volunteer Experience

01/2020 – 01/2021

- Referent AIRicerca Denmark Chapter, Copenhagen - Denmark
AIRicerca is an association of Italian researchers aiming at promoting networking, scientific collaborations, exchange of professional information and public outreach (<https://airicerca.org/>).