

Mohammad Yaghini

✉ mohammad.yaghini@mail.utoronto.ca

 [myaghini](#)

 [m-yaghini](#)

 [m-yaghini.github.io](#)

PhD Student in ML, Data Scientist

Education

- Sept.2020 – **Ph.D. in Machine Learning**, *University of Toronto and Vector Institute*, Canada, CleverHans Lab
Present (under the supervision of Prof. Nicolas Papernot)
- Sept.2017 – **Master's in Data Science**, *School of Computer and Communication Sciences*, École Polytechnique
Oct.2019 Fédérale de Lausanne (EPFL), Switzerland, GPA: 5.26/6
Thesis: A Human-in-the-loop Framework to Construct Context-dependent Mathematical Formulations of Fairness
- Sept.2016 – **Master's in Communication Systems**, *School of Computer and Communication Sciences*, École
Aug.2017 Polytechnique Fédérale de Lausanne, Switzerland – switched to Data Science in the 2nd year.
- 2011–2016 **B.Sc. in Electrical Engineering – Communications**, *Isfahan University of Technology (IUT)*,
Iran, GPA: 18.37/20, GPA (junior and senior): 18.66/20
Thesis: An Energy-Efficient Cooperative Mechanism for Device-to-Device Communications

Publications

- * Joint 1st authors Hengrui Jia*, **M. Yaghini***, Christopher A. Choquette-Choo, Natalie Dullerud, Anvith Thudi, Varun Chandrasekaran, and Nicolas Papernot. Proof-of-learning: Definitions and practice. *To appear in the 42nd IEEE Symposium on Security and Privacy (Oakland)*, 2021.
- Pratyush Maini, **M. Yaghini**, and Nicolas Papernot. Dataset Inference: Ownership Resolution in Machine Learning. In *Proceedings of the 2021 International Conference on Learning Representations (ICLR 2021)*, 2021.
- M. Yaghini**, Hoda Heidari, and Andreas Krause. A Human-in-the-loop Framework to Construct Context-dependent Mathematical Formulations of Fairness. *arXiv e-prints*, page arXiv:1911.03020, Nov 2019.
- M. Yaghini**, K. Bogdan, and C. Troncoso. Disparate Vulnerability: on the Unfairness of Privacy Attacks Against Machine Learning. *arXiv e-prints*, page arXiv:1906.00389, Jun 2019.
- Naman Goel, **M. Yaghini**, and Boi Faltings. Non-Discriminatory Machine Learning Through Convex Fairness Criteria. In *Proceedings of the Thirty-Second AAAI Conference on Artificial Intelligence, (AAAI-18)*, pages 3029–3036, 2018.

Experience

Research Assistant

- Sep.2020– **CleverHans Lab**, UoT/Vector Institute
Present
 - Trustworthy Machine Learning
 - Intellectual Property of ML Models
 - ML Security for Audio Domain
- March.2020– **Privacy and Trust Group**, *Reza Shokri*, NUS (remote)
Present
 - Human-in-the-loop Explainable ML
- Mar.2019– **Learning and Adaptive Systems (LAS)**, *Andreas Krause*, ETH Zurich
- August.2019
 - Master thesis on context-dependent mathematical formulations of fairness
- Oct.2017– **Security and Privacy Engineering Laboratory (SPRING)**, *Carmela Troncoso*, EPFL
Dec.2019
 - Quantifying privacy vulnerability and its disparity for ML models, defenses, and the trade-offs
- Feb.2018– **Data Science Lab (DLAB)**, *Robert West*, EPFL
Jun.2018
 - Designing mechanisms for truthful judgment aggregation to detect misinformation
- Feb.2017– **Artificial Intelligence Laboratory (LIA)**, *Boi Faltings*, EPFL
Aug.2017
 - Building a convex fairness metric for classifiers
- Sep.2014– **Game Theory & Mechanism Design Research Grp. (GTMD)**, *MohammadHossein Manshaei*
Aug.2016
 - Designing a game-theoretic mechanism to incentivize device-to-device communication for 5G networks

Industry Experience

- Sept.2018– **Expedia**, *Junior Data Scientist*, Geneva
Feb.2019 ○ Building statistical models for advanced time-series forecasting using Spark

Voluntary Work

- July.2017– **EPFL Iranian Student Association (IRSA)**, *Public Relations*, Lausanne
June.2018 ○ Moderating bi-weekly intellectual discussions on society, culture, technology, psychology, etc.

Notable Student Projects

- | | | |
|-----------|--|------------------------------------|
| Jul. 2018 | Defending Against Membership Attacks on ML Models | <i>ML Security, Deep Learning</i> |
| May 2018 | Symmetric Autoencoder for Text Classification | <i>Deep Learning, NLP</i> |
| Jun. 2018 | Empirical Mechanism Design for Crowd-Sourced Fact-Checking | <i>NLP, Mechanism Design</i> |
| Dec. 2017 | Evolution of Swiss Broadcasts in the Course of 20th Century ↗ | <i>Data Analysis/Visualization</i> |
| June 2017 | Fair Machine Learning | <i>Machine Learning in society</i> |
| May 2017 | EPFL Electricity Consumption Forecasting Challenge (1st Place) | <i>Time Series Forecasting</i> |
| Jul. 2015 | Optimizing Popular Content Distribution in Cellular D2D Networks | <i>Mechanism Design</i> |

Related Course Work

- | | |
|--|--|
| ○ Machine Learning | ○ Differential Privacy |
| ○ Game Theory and Multi-agent Systems | ○ Information Theory & Signal Processing |
| ○ Algorithms for Private Data Analysis | ○ Deep Learning |
| ○ Convex Optimization | ○ Data Visualization |

Computer Skills

- | | | | |
|---------------|-------------------------------------|--------------|--|
| Machine Lear. | Scikit, Pandas, Spark MLib, XGBoost | Languages | Python, Scala, Julia, MATLAB, Java, Javascript/Typescript, C |
| Deep Lear. | PyTorch, Keras | Big Data | Spark, Hive SQL, Kafka/SparkStreaming |
| Data Vis. | Plotly, D3.js, Matplotlib | Optimization | CVX, CVXOPT |
| Web Dev. | JS/TS, HTML, CSS, React | NLP | NLTK, Gensim |

Languages and Test Scores

- | | |
|--|--|
| Persian Native proficiency | English Full proficiency |
| French Full proficiency (DELF B2: 76.5/100) | TOEFL iBT Total: 109/120, Reading: 29/30, |
| Turkish Speaking proficiency | Writing: 27/30, Listening: 29/30, Speak.: 24/30 |

Awards and Honors

- 2019–2020 Received **Ph.D.** offers from UoT/Vector Institute (Toronto, CA), EPFL (Lausanne, CH), MPI-SWS (Saarbrücken, DE), UCL (London, UK), and NUS (Singapore, SG)
- 2016 Received **Direct-Ph.D.** offers from University of Michigan (Ann Arbor, US), University of Pennsylvania, and Virginia Tech (Blacksburg, US)
- 2016 Received **Master's** offers from EPFL (Lausanne, CH), ETHZ (Zurich, CH), University of British Columbia (Vancouver, Canada)
- 2011–2016 Received **Gifted Student Award** (Sept. 2011) and **Merit-based admission** to MSc program in Communication Systems (Dec. 2014), Isfahan University of Technology
- Jun. 2015 **Ranked 7th** (in the top 8%) among 92 ECE undergraduates and **3rd** among 27 communications engineering students, class of 2011
- 2011 Ranked in the **top 0.3% (99.6 percentile)** among 252,000 participants in the Nationwide University Entrance Exam, also known as *Concours* (Math-Physics)

References

- **Nicolas Papernot**, Assistant Professor, University of Toronto nicolas.papernot@utoronto.ca
- **Carmela Troncoso**, Assistant Professor, SPRING, EPFL carmela.troncoso@epfl.ch