Michele Minelli

Personal Data

Place and Date of Birth:	Parma, Italy | 25 December 1992
e-mail:	micheleminelli1@gmail.com
web page:	http://www.di.ens.fr/~minelli/
Skype ID:	michele.minelli2
LinkedIn:	https://www.linkedin.com/in/mminelli

Work Experience

2018 –	**Alten**, Nice, France IT Consultant
Feb. 2017 – Jul. 2017	**CryptoExperts**, Paris, France. Internship on implementation of Fully Homomorphic Encryption schemes. Supervisors: Pascal Paillier and Louis Goubin

Education

2015 – 2018 **Ph.D. in Computer Science - Cryptography**
Crypto Team – École normale supérieure, Paris, France.
Research topic: "Fully Homomorphic Encryption for Machine Learning".
Supervisors: Michel Abdalla and Hoeteck Wee

2013 – 2015 **Master's Degree in Computer Engineering**, University of Parma, Parma, Italy.
Final grade: **110/110 *cum laude***
Thesis title: "Deep learning techniques for recognizing emotions in face images".
Advisor: Prof. Stefano Cagnoni

2010 – 2013 **Bachelor's Degree in Computer Engineering**, University of Parma, Parma, Italy.
Final grade: **110/110 *cum laude***
Thesis title: "TrackShot Golf: mobile application for the statistical analysis of golfers' performance".
Advisor: Prof. Stefano Cagnoni

2005 – 2010 **Diploma di maturità scientifica**, Liceo Scientifico "Giacomo Ulivi", Parma, Italy.
Final grade: **100/100 *cum laude***

Languages

Italian:	Mother tongue
English:	Full professional proficiency
French:	Basic oral proficiency

Computer Skills

Advanced knowledge:	Windows, Microsoft Office, linux, LaTeX, html, git, svn
Programming languages:	C, C++, Java (also for Android development), Python, Vb.Net, Matlab
Basic knowledge:	php, mySQL

Publications

1. **Lattice-Based zk-SNARKs from Square Span Programs**
   with Rosario Gennaro, Michele Orrù, and Anca Nitulescu
   ACM CCS 2018, ePrint (https://eprint.iacr.org/2018/275)
2. **Fast Homomorphic Evaluation of Deep Discretized Neural Networks**
   with Florian Bourse, Matthias Minihold, and Pascal Paillier
   CRYPTO 2018, ePrint (https://eprint.iacr.org/2017/1114)
3. **Processing Encrypted Data Using Homomorphic Encryption**
   with Anthony Barnett, Charlotte Bonte, Carl Bootland, Joppe W. Bos, Wouter Castryck, Anamaria Costache, Louis Goubin, Ilia Iliashenko, Tancrède Lepoint, Pascal Paillier, Nigel P. Smart, Frederik Vercauteren, Srinivas Vivek, and Adrian Waller
   Workshop on Data Mining with Secure Computation, SODA project, 2017
4. **FHE Circuit Privacy Almost For Free**
   with Florian Bourse, Rafaël Del Pino, and Hoeteck Wee
   CRYPTO 2016, ePrint (http://eprint.iacr.org/2016/381)

Talks and Presentations

1. **Privacy-Preserving Neural Networks**
   ECRYPT-NET School on Integrating Advanced Cryptography with Applications
   16-21/09/2018, Kos, Greece
2. **Fast Homomorphic Evaluation of Deep Discretized Neural Networks**
   CRYPTO 2018
   19-23/08/2018, University of California Santa Barbara
3. **Automated Detection of Organized Crime Through Fully Homomorphic Encryption**
   ECRYPT-NET School on Correct and Secure Implementation
   8-12/10/2017, Crete, Greece

4. **Increased efficiency and functionality through lattice-based cryptography**
   ECRYPT-NET Cloud Summer School
   19-23/09/2016, KU Leuven, Leuven, Belgium

5. **FHE Circuit Privacy Almost For Free**
   3rd Paris Crypto Day
   06/09/2016, INRIA, Paris, France

Scholarships and Certificates

3 years (2015 – 2018)	Researcher within EU-financed ECRYPT-NET project (Horizon 2020 programme)
5 years (2011 – 2015)	Scholarship of the University of Parma
5 years (2007 – 2011)	Winner of a scholarship offered by BPER (*Banca Popolare dell'Emilia Romagna*)
5 years (2007 – 2011)	Winner of a scholarship offered by Emilia Romagna region

Interests and Activities

- IT security
- software engineering
- programming
- artificial intelligence
- golf
- traveling
- chess
- music