

# Florian Tramèr

720 Serra Street, Apt. 516, Stanford, CA 94305

✉ [tramer@cs.stanford.edu](mailto:tramer@cs.stanford.edu)

🌐 <http://www.floriantramer.com>

🌐 <http://www.linkedin.com/in/floriantramer>

📄 <https://scholar.google.com/citations?user=ijH0-a8AAAAJ&hl=en>

☎ +1-650-250-6336

## EDUCATION

---

- Sep. 2016 - Today      **PhD in Computer Science** - STANFORD UNIVERSITY, Stanford CA, USA  
Advised by Prof. Dan Boneh
- Sep. 2013 - Aug. 2015      **Master in Computer Science** - EPFL, Lausanne, Switzerland  
Thesis: “Algorithmic Fairness Revisited”, supervised by Prof. Jean-Pierre Hubaux  
Specialization in *Internet Computing*  
GPA: 5.9/6.0
- Sep. 2009 - Aug. 2012      **Bachelor in Computer Science** - EPFL, Lausanne, Switzerland  
Exchange year (2011-2012) - CARNEGIE MELLON UNIVERSITY, Pittsburgh PA, USA  
GPA: 5.8/6.0

## PROFESSIONAL EXPERIENCE

---

- Jun. 2017 - Sep. 2017      **IBM RESEARCH** - *Research Intern*, Yorktown Heights, NY, USA  
Supervised by Dr. Evelyn Duesterwald
- Study of *adversarial examples* for speech recognition systems.
- Sep. 2015 - Aug. 2016      **EPFL** - *Scientific Assistant*, Lausanne, Switzerland
- Study of *extraction attacks* on Machine-Learning-as-a-Service platforms [TZJ+16].
  - Formal analysis of *trusted execution environments* [PST17], in particular for *transparent enclaves*, a model of trusted hardware with arbitrary side-channel leakage [TZL+17].
  - Design of formal methodologies and a tool, *FairTest*, for the discovery of “discrimination bugs” in data-driven algorithms [TAG+17].
  - Research on privacy-preserving ride-hailing [PDJ+17] and genomic studies [THH+15].
- Supervised by Prof. J-P. Hubaux, Laboratory for Communications and Applications.
- Sep. 2013 - Feb. 2015      **EPFL** - *Research Assistant*, Lausanne, Switzerland  
Implementation and complexity analysis of algorithms for solving hard learning problems such as Learning Parity with Noise [BTV16], Learning with Errors and Learning with Rounding [DTV15].  
Supervised by Prof. S. Vaudenay, Laboratory for Cryptography and Security.
- Mar. 2013 - Aug. 2013      **ELCA** - *Security Intern*, Lausanne, Switzerland  
Design, proof of concept and implementation of a proxy web-application integrating the Elcard strong-authentication mechanism with the SAML 2.0 standard. Acquired experience with federated identity solutions, strong authentication methods, J2EE web development and software testing (unit, integration, regression). The new functionality is to be added to the next Elcard release.

## PROFESSIONAL SERVICE

---

### Program committee.

- Machine Learning and Computer Security Workshop (co-located with NIPS), 2017

### Peer reviewer.

- Financial Cryptography and Data Security, 2018
- IEEE Symposium on Security & Privacy, 2017
- Privacy Enhancing Technologies Symposium, 2016

## AWARDS AND SCHOLARSHIPS

---

2016		<b>ZDENEK AND MICHAELA BAKALA FOUNDATION FELLOWSHIP</b>
2015		<b>EPFL MASTER AWARD</b> (Highest GPA for complete Master studies at EPFL) <b>SIA VAUDOISE AWARD</b> (Highest GPA in Engineering) <b>ELCA AWARD</b> (Highest GPA in Computer Science)
2013-2015		<b>EPFL EXCELLENCE FELLOWSHIP</b> (Awarded for outstanding academic records)
2013-2015		<b>EPFL RESEARCH SCHOLARS MSc Program</b>
2012		<b>EPFL BACHELOR PRIZE</b> (Highest GPA for complete Bachelor studies: 3 <sup>rd</sup> place)
2012		<b>CMU COMPUTER SCIENCE DEAN'S LIST</b> (GPA: 4.0/4.0)

## LANGUAGES

---

<b>French</b>	Native language
<b>English</b>	Fluent - CEFR level C2, Certificate in Advanced English - ESOL (2009)
<b>German</b>	Fluent - CEFR level C2

## TECHNICAL SKILLS

---

<b>Programming</b>	Java, Scala, C, Python Matlab, x86 Assembly, J2EE, Web Development	very good skills good skills
<b>Machine Learning</b>	TensorFlow, Theano, Keras, Scikit-Learn	
<b>Systems</b>	Unix, Windows, OS X environments Tomcat, Apache Httpd, Adfs 2.0, SQL, Hadoop, HBase, Svn, Git	

## PUBLICATIONS

---

### Journal Articles

- [RTJ+17] J. L. Raisaro, F. Tramèr, Z. Ji, D. Bu, Y. Zhao, K. Carey, et al. "Addressing Beacon Re-Identification Attacks: Quantification and Mitigation of Privacy Risks". *Journal of the American Medical Informatics Association (JAMIA)* (Feb. 2017).

- [BTV16] S. Bogos, F. Tramèr, and S. Vaudenay. “On Solving LPN using BKW and Variants”. *Cryptography and Communications* 8.3 (July 2016), pp. 331–369.

## Conference Proceedings

- [TKP+18] F. Tramèr, A. Kurakin, N. Papernot, I. Goodfellow, D. Boneh, and P. McDaniel. “Ensemble Adversarial Training: Attacks and Defenses”. In *International Conference on Learning Representations (ICLR)*. <https://arxiv.org/abs/1705.07204>. Dec. 2018.
- [PDJ+17] A. Pham, I. Dacosta, B. Jacot-Guillarmod, K. Huguenin, T. Hajar, F. Tramèr, and J.-P. Hubaux. “PrivateRide: A Privacy-Preserving and Secure Ride-Hailing Service”. In *Privacy Enhancing Technologies Symposium (PETS)*. July 2017.
- [PST17] R. Pass, E. Shi, and F. Tramèr. “Formal Abstractions for Attested Execution Secure Processors”. In *EUROCRYPT*. Apr. 2017.
- [TAG+17] F. Tramèr, V. Atlidakis, R. Geambasu, D. Hsu, J.-P. Hubaux, M. Humbert, A. Juels, and H. Lin. “FairTest: Discovering Unwarranted Associations in Data-Driven Applications”. In *IEEE European Symposium on Security and Privacy (EuroS&P)*. IEEE. Apr. 2017.
- [TZL+17] F. Tramèr, F. Zhang, H. Lin, J.-P. Hubaux, A. Juels, and E. Shi. “Sealed-Glass Proofs: Using Transparent Enclaves to Prove and Sell Knowledge”. In *IEEE European Symposium on Security and Privacy (EuroS&P)*. IEEE. Apr. 2017.
- [TZJ+16] F. Tramèr, F. Zhang, A. Juels, M. Reiter, and T. Ristenpart. “Stealing Machine Learning Models via Prediction APIs”. In *USENIX Security Symposium*. Aug. 2016.
- [THH+15] F. Tramèr, Z. Huang, J.-P. Hubaux, and E. Ayday. “Differential Privacy with Bounded Priors: Reconciling Utility and Privacy in Genome-Wide Association Studies”. In *ACM Conference on Computer and Communications Security (ACM CCS)*. ACM. Oct. 2015, pp. 1286–1297.
- [DTV15] A. Duc, F. Tramèr, and S. Vaudenay. “Better Algorithms for LWE and LWR”. In *EUROCRYPT*. Springer, Apr. 2015, pp. 173–202.

## Manuscripts

- [BDT+17] L. Breidenbach, P. Daian, F. Tramèr, and A. Juels. *Enter the Hydra: Towards Principled Bug Bounties and Exploit-Resistant Smart Contracts*. Cryptology ePrint Archive, Report 2017/1090. <http://eprint.iacr.org/2017/1090>. Nov. 2017.
- [TPG+17] F. Tramèr, N. Papernot, I. Goodfellow, D. Boneh, and P. McDaniel. *The Space of Transferable Adversarial Examples*. arXiv preprint arXiv:1704.03453. <https://arxiv.org/abs/1704.03453>. Apr. 2017.