Florian Tramèr

720 Serra Street, Apt. 516
Stanford, CA 94305
✉ florian.tramer@gmail.com
linkedin.com/in/floriantramer
☎ +1-650-250-6336

Strong Skills

- Cryptography, Privacy, Machine Learning, Theory
- Broad mathematical background, strong research interests
- Excellent linguistic skills in English, French and German

Education

2016- **PhD in Computer Science** - Stanford University, Stanford CA, USA

2013-2015 **Master in Computer Science** - EPFL, Lausanne, Switzerland
Thesis: "Algorithmic Fairness Revisited"
Specialization in *Internet Computing*
GPA: 5.9/6.0

2009-2012 **Bachelor in Computer Science** - EPFL, Lausanne, Switzerland
Exchange year (2011-2012) - Carnegie Mellon University, Pittsburgh PA, USA
GPA: 5.8/6.0

Professional Experience

2015-2016 **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 services [PDJ+17] and genomic studies [THH+15].

Supervised by Prof. J-P. Hubaux, Laboratory for Communications and Applications.

2013-2015 **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.

2013 (5 months) **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.

Languages

French Native language
English Fluent - Cefr level C2, Certificate in Advanced English - Esol (2009)
German Fluent - Cefr level C2

Technical Skills

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

Awards and Scholarships

2016	**Zdenek and Michaela Bakala Foundation Fellowship**
2015	**EPFL Master Award** (Highest GPA for complete Master studies at EPFL) **SIA Vaudoise Award** (Highest GPA in Engineering) **Elca Award** (Highest GPA in Computer Science)
2013-2015	**EPFL Excellence Fellowship** (Awarded for outstanding academic records)
2013-2015	**EPFL Research Scholars MSc Program**
2012	**EPFL Bachelor Prize** (Highest GPA for complete Bachelor studies: 3rd place)
2012	**CMU Computer Science Dean's List** (GPA: 4.0/4.0)

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

[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 *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 *EuroS&P*. 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 *EuroS&P*. 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

[TKP+17] F. Tramèr, A. Kurakin, N. Papernot, D. Boneh, and P. McDaniel. *Ensemble Adversarial Training: Attacks and Defenses*. May 2017.

[TPG+17] F. Tramèr, N. Papernot, I. Goodfellow, D. Boneh, and P. McDaniel. *The Space of Transferable Adversarial Examples*. Apr. 2017.