ACADEMIC CURRICULUM VITAE – LUCCA HIRSCHI

PERSONAL INFORMATION

Lucca Hirschi
ETH Zürich
Universitätstrasse 6
8092 Zürich
lucca.hirschi@ens-lyon.org
www.lsv.ens-cachan.fr/~hirschi/

I am a postdoctoral researcher at ETH Zürich in the Prof. David Basin's group. My research interests mainly focus on *formal methods* for *security* and *privacy*. I generally enjoy research projects that combine both foundational contributions and practical applications.

I did my Ph.D at Ecole Normale Supérieure de Cachan jointly advised by Stéphanie Delaune and David Baelde.

EDUCATION

(06/2017-) — **PostDoc** at ETH Zurich in the Prof. David Basin's group (Information Security Group).

(09/2013-05/2017) — **Ph.D** at LSV, Ecole Normale Supérieure de Cachan under the supervision of Stéphanie Delaune and David Baelde. Thesis title : *Automated Verification of Privacy in Security Protocols : Back and Forth Between Theory & Practice*.

(09/2010-09/2013) — **Bachelor & Master of Science Degree in Theoretical Computer Science** at Ecole Normale Supérieure de Lyon (university level institution training teachers and researchers, entrance to which is based on a competitive exam), Lyon, France.

(09/2008-09/2010) — **Classes préparatoires scientifiques** at Lycée du Parc (post-secondary preparatory classes in science for competitive entrance exams), Lyon, France.

PUBLICATIONS

C. Cremers and L. Hirschi. *Improving Automatic Symbolic Analysis for E-voting Protocols : Sufficient Conditions for Ballot Secrecy.* Under submission.

R. Borgaonkar, L. Hirschi, A. Martin, S. Park, J.-P. Seifert and A. Shaik. *New AKA Privacy Attacks in 4G Networks.* Under submission. Associated **Black Hat USA'17** briefing.

D. Baelde, S. Delaune and L. Hirschi. *A Reduced Semantics for Deciding Trace Equivalence.* Accepted in **Logical Methods in Computer Science**.

Piers O'Hanlon, Ravishankar Borgaonkar and Lucca Hirschi. *Mobile subscriber WiFi privacy.* Accepted at **MoST'17** (S&P Workshops) (**best paper award**). 2017. To appear.

S. Delaune and L. Hirschi. *A survey of symbolic methods for establishing equivalence-based properties in cryptographic protocols.* In **Logic and Algebraic Programming** 87, pages 127-144. Elsevier, 2016.

A. Doumane, D. Baelde, L. Hirschi and A. Saurin. *Towards Completeness via Proof Search in the Linear Time μ-calculus.* In **LICS'16**, pages 377-386. ACM Press, 2016.

L. Hirschi, D. Baelde and S. Delaune. *A method for verifying privacy-type properties : the unbounded case.* In **S&P'16**, pages 564-581. IEEECSP, 2016

D. Baelde, S. Delaune and L. Hirschi. *Partial Order Reduction for Security Protocols.* In **CONCUR'15**, Leibniz International Proceedings in Informatics 42, pages 497-510. Leibniz-Zentrum für Informatik, 2015.

D. Baelde, S. Delaune and L. Hirschi. *A reduced semantics for deciding trace equivalence using constraint systems.* In **POST'14**, LNCS 8414, pages 1-21. Springer, 2014.

OTHER PUBLICATIONS

L. Hirschi and S. Delaune. *Description of some case studies.* Deliverable VIP 6.1, (ANR-11-JS02-0006), 2013.

GRANTS

2016 — Grant by European Cooperation in Science and Technology (Crypto Action) for visiting Professor Cas Cremers at University of Oxford. Additional mobility support grant from my doctoral school.

TEACHING ASSISTANT

2017 (22.5h) — Logic (tutorial classes).
2016 (30h) — Software engineering.
2016 (22.5h) — Projects around Logic : SAT (logical cryptanalysis of MD5) and Coq.
2016 (22.5h) — Logic (tutorial classes).
2015 (22.5h) — Computability (tutorial classes).
2014,2015 ($2 * 11$h) — Introduction to the Coq Proof Assistant.
2013,2014,2016 ($2 * 45 + 12$h) — Computer Programming : C, OCaml, compiler project (lab classes).

TOOLS & SOFTWARE

UKano — Automatic verifier of unlinkability and anonymity for a large class of 2-agents protocols (in OCaml, $\approx$ 2 kloc).
POR for APTE — Implementation of Partial Order Reduction techniques in APTE (in OCaml, $\approx$ 3 kloc). Implementation of similar techniques in the tool SPEC (in Bedwyr, $\approx$ 3.3 kloc).

TECHNICAL SKILLS

OCaml, C, Python, C++, Haskell, assembly (x86, mips). Knowledge in logic programming.

PARTICIPATION TO CONFERENCES & SCHOOLS

Conferences — Troopers'17, S&P'16 (Oakland), POST'16 (ETAPS), CONCUR'15, CSF'15, POST'15, JFLA'15, LICS&CSF'15 (VSL), POST'14 (ETAPS).

Schools — EPIT'15 (École « Preuve mécanisée de programmes »),
— The Joint EasyCrypt-F*-CryptoVerif School (2014),
— 13th & 14th International School on Foundations of Security Analysis and Design (2013 & 2014).

Workshops — Logic and Verification Methods in Security and Privacy (NII Shonan Meeting Seminar) (2015), Workshop on Abella and Bedwyr at LIX (2012).

SOME TALKS

2017 — **Invited talk** at Troopers'17 (with R. Borgaonkar), **invited talk** at GSMA Fraud & Security.
2016 — Security & Privacy (Oakland), HotSpot (ETAPS), InfSec group seminar at ETHZ, 68NQRT Seminar (IRISA & INRIA Rennes).
2015 — Logic and Verification Methods in Security and Privacy (NII Shonan Meeting Seminar 069), CONCUR, CSF.
2014 — Seminar Chocola (ENS Lyon), POST (ETAPS), Seminar CEA-LIST (CEA Saclay).

2013 — 13th International School on Foundations of Security Analysis and Design, Popularization talk at Fête de la Science (science fair) at ENS Cachan.
2012 — Workshop on Abella and Bedwyr at LIX.

VISITING & INTERNSHIPS

2016 — 3 months-academic visit at University of Oxford with Professor Cas Cremers. The two collaborations started there with respectively Cas Cremers and Ravishankar Borgaonkar resulted in two papers under submissions.
2013 — 4 months-internship about reduction of interleavings for trace equivalence checking of security protocols with David Baelde & Stéphanie Delaune, LSV, ENS Cachan.
2012 — 2 months-internship about alternating automata for XPath queries directed by Kim Nguyên, LRI lab, Paris-Sud.
— 3 months-internship about infinite and cyclic proofs and Büchi automata directed by David Baelde, PLS lab, IT University of Copenhagen, Denmerk.
2011 — 6 weeks-internship about type-safe language for XML directed by Giuseppe Castagna and Kim Nguyên, PPS lab, Paris-7.

PROJECTS & REVIEWS

Participation to projects : ANR project Sequoia, ANR project ProSe, ANR JCJC project VIP.
I have reviewed papers for CCS, POST (ETAPS), the Journal of Computer Security and the journal LNCS Transactions on Petri Nets and Other Models of Concurrency.

ADMINISTRATIVE TASKS

I was organizing the monthly internal seminar of my group at LSV, ENS Cachan (2015-2017). I helped organizing the Workshop on the 20th Anniversary of LSV (2017). I helped organizing the Colloquium in honour of Martin Abadi (2015).

MISCELLANEOUS

I do enjoy a lot rock climbing, hiking & skiing.