# ACADEMIC CURRICULUM VITAE – LUCCA HIRSCHI

## PERSONAL INFORMATION

Lucca Hirschi
Inria Nancy - Grand Est
615 rue du jardin botanique
54600 Villers lès Nancy
lucca.hirschi@inria.fr
https://members.loria.fr/LHirschi/
*Born on 10/03/1990, 1 child (21/01/2019)*

I am a researcher at Inria and LORIA, member of the PESTO team. My research interests mainly focus on *formal methods* for *security* and *privacy*. I design new verification techniques, algorithms, and tools to effectively and efficiently analyze formal security properties. I generally enjoy research projects that combine both theoretical contributions and practical applications, including analyzing real-world cryptographic protocols. More recently, I also took a great interest in fuzz testing techniques.

## EMPLOYMENT

• (01/2019-) — **Research scientist (tenured, full-time research position)** at Inria in the Pesto team in the lab LORIA, France.

• (06/2017-12/2018) — **Postdoc researcher & teaching assistant** at ETH Zurich in the David Basin's *Information Security Group*, Switzerland.

• (09/2013-05/2017) — **Ph.D. student & teaching assistant** at Ecole Normale Supérieure de Paris-Saclay, France.

## EDUCATION

• (09/2013-05/2017) — **Ph.D. in Computer Science** titled *Automated Verification of Privacy in Security Protocols : Back and Forth Between Theory & Practice* at Ecole Normale Supérieure de Paris-Saclay, France advised by Stéphanie Delaune and David Baelde.
→ ***Best thesis 2017 prize*** *by* GDR Sécurité *(main, nation-wide research network on security in France created by the French state research organization (CNRS)).*

• (09/2010-09/2013) — **Bachelor & Master of Science Degree in Theoretical Computer Science with honours** at Ecole Normale Supérieure de Lyon, France.
→ *Ecole Normale Supérieure (ENS) schools are among the most prestigious French "Grandes Écoles'.*

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

## PUBLICATIONS IN INTERNATIONAL PEER-REVIEWED JOURNALS

Jannik Dreier, Lucca Hirschi, Saša Radomirovic, and Ralf Sasse. *Verification of Stateful Cryptographic Protocols with Exclusive OR.*
In **Journal of Computer Security (JCS)** (special issue of CSF'18), 2020.

L. Hirschi, D. Baelde, and Stéphanie Delaune. *A method for unbounded verification of privacy-type properties.*
In **Journal of Computer Security (JCS)**, 2019.

D. Baelde, S. Delaune, and L. Hirschi. *A Reduced Semantics for Deciding Trace Equivalence.*
In journal of **Logical Methods in Computer Science (LMCS)** 13, issue 2. Episciences, 2017.

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

PUBLICATIONS IN INTERNATIONAL PEER-REVIEWED CONFERENCES

M. Ammann, L. Hirschi, S. Kremer. *DY Fuzzing : Formal Dolev-Yao Models Meet Protocol Fuzz Testing.*
In **S&P'24**, 2024.

A. Debant, L. Hirschi. *Reversing, Breaking, and Fixing the French Legislative Election E-Voting Protocol.*
In **Usenix Security'23**, 2023.

V. Cheval, C. Cremers, A. Dax, L. Hirschi, C. Jacomme, S. Kremer. *Hash Gone Bad : Automated discovery of protocol attacks that exploit hash function weaknesses.*
In **Usenix Security'23**, 2023. **Best paper award.**

L. Hirschi, L. Schmid, D. Basin. *Fixing the Achilles Heel of E-Voting : The Bulletin Board.*
In **CSF'21**, IEEE, 2021.

G. Girol, L. Hirschi, R. Sasse, D. Jackson, C. Cremers, and D. Basin. *A Spectral Analysis of Noise : A Comprehensive, Automated, Formal Analysis of Diffie-Hellman Protocols.*
In **Usenix Security'20**, 2020.

L. Hirschi and C. Cremers. *Improving Automatic Symbolic Analysis for E-voting Protocols : Sufficient Conditions for Ballot Secrecy.*
In **Euro S&P'19**, IEEE, 2019.

R. Borgaonkar, L. Hirschi, S. Park, A. Shaik. *New Privacy Threat on 3G, 4G, and Upcoming 5G AKA Protocols.*
In **PETS'19**. Associated proposal of briefing accepted at **Black Hat USA'17**.

D. Basin, J. Dreier, L. Hirschi, S. Radomirovic, R. Sasse, and V. Stettler. *A Formal Analysis of 5G Authentication.*
In **CCS'18**, ACM, 2018.

D. Baelde, S. Delaune, and L. Hirschi. *POR for Security Protocol Equivalences : Beyond Action-Determinism.*
In **ESORICS'18**, Springer, 2018.

Jannik Dreier, Lucca Hirschi, Saša Radomirovic, and Ralf Sasse. *Automated Unbounded Verification of Stateful Cryptographic Protocols with Exclusive OR.*
In **CSF'18**, IEEE, 2018.

A. Doumane, D. Baelde, L. Hirschi, and A. Saurin. *Towards Completeness via Proof Search in the Linear Time $\mu$-calculus.*
In **LICS'16**, ACM/IEEE, 2016.

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

D. Baelde, S. Delaune, and L. Hirschi. *Partial Order Reduction for Security Protocols.*
In **CONCUR'15**, 2015.

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

PUBLICATIONS IN INTERNATIONAL PEER-REVIEWED WORKSHOPS

D. Basin, L. Hirschi, R. Sasse. *Symbolic Analysis of Identity-Based Protocols.*

In **CathyFest Workshop**, LNCS 11565. Springer, 2019.

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

OTHER PUBLICATIONS

L. Hirschi, R. Sasse, and J. Dreier. *Security Issues in the 5G Standard and How Formal Methods Come to the Rescue.*
**ERCIM News**, issue 117, 2019.

X. Bonnetain, A. Canteaut, V. Cortier, P. Gaudry, L. Hirschi, S. Kremer, S. Lacour, M. Lequesne, G. Leurent, L. Perrin, A. Schrottenloher, E. Thomé, S. Vaudenay, C. Vuillot. *Le traçage anonyme, dangereux oxymore : Analyse de risques à destination des non-spécialistes.*
Preprint in 2020. The publication of this document was followed by multiple interviews (Le Monde, Les Echos, Le Figaro, Télérama, AEF, France Culture, ...).

WORKS NOT YET PUBLISHED

L. Hirschi. *Symbolic Abstractions for Quantum Protocol Verification.*

GRANTS, PRIZES, COMPETITIVE SELECTIONS

2023 — **Best paper award** at Usenix Security 2023 for *Hash Gone Bad : Automated discovery of protocol attacks that exploit hash function weaknesses*.
2022 — My *ProtoFuzz* project (2023-2027) **was funded by the ANR (280k €)** as a *JCJC project* (individual research projects coordinated by young researchers).
2019 — One of the finalists of the 2019 ERCIM Cor Baayen Young Researcher Award.
— Holder of the "Prime d'encadrement doctoral et de recherche" (PEDR) from 2020 to 2024. → *This is a bonus given by my institution for* ***high-standard research*** *(ca. 10% of researchers benefit from this bonus).*
2018 — Got included in the **GSMA Hall of Fame** (CVD-2018/0012) that "recognises and acknowledges the positive impact [I have had] on the mobile industry" (GSMA is an international consortium of the most important mobile industry actors).
— **Best thesis 2017 prize** awarded by *GDR Sécurité*, which is the main, nation-wide research network on security in France, initiated by the French state research organization.
2017 — Accepted briefing proposal at **Black Hat USA'17** (highly selective) about our work on privacy attacks in mobile telephony (later presented in *New Privacy Threat on 3G, 4G and incoming 5G AKA Protocol* at PETS'19).
— **Best paper award** at MoST'17 (Mobile Subscriber WiFi Privacy at *IEEE Security and Privacy Workshops*) for our *Mobile subscriber WiFi privacy* paper.
2016 — Accepted mobility grants for my research proposal I wrote as a Ph.D. student (European COST Grant by European Cooperation in Science and Technology (Crypto Action) + Doctoral School Paris-Saclay) for visiting Professor Cas Cremers at University of Oxford (3 month academic visit).

INVITED TALKS AND LECTURES

2023 — **Invited talk** at the Apple Tech Talks (invited by Yann Oddos) about formal methods and DY fuzzing.
2023 — **Invited talk** at the annual workshop of the **GDR Sécurité** (main, nation-wide research network on security in France).
2023 — **Contributed talk** at the Real World Cryptography conference (chosen by the Program Committee).
2021 — **Invited lecture** at the summer school of the **GDR IM** (main, national research network on theoretical computer science).
— **Invited lecture** at the winter school of the **GDR Sécurité**.

2019 — **Invited talk** at the annual workshop of the **GDR Sécurité**.
2018 — **4 days lecture at Huawei Singapore Research Center**, Singapore, 2018.
2017 — **Invited talk** at the conference **Troopers'17** (shared with R. Borgaonkar) about our *New Privacy Threat on 3G, 4G, and Upcoming 5G AKA Protocols* paper.
— **Invited talk** at **GSMA Fraud & Security** meeting presenting the same work.
2015 — **Invited talk** at NII Shonan Meeting 069 - Logic and Verification Methods in Security and Privacy (Dagstuhl-like Seminars in Japan).

SERVICE & PROJECTS

— I am the **PI** of the ProtoFuzz project (2023-2027) funded by **ANR JCJ** (280k €).
— I serve in the **program committee** of the **European Symposium on Research in Computer Security** (ESORICS) **2024–now** and of the **HotSpot workshop** (yearly workshop since 2015, affiliated with IEEE European Symposium on Security and Privacy) **2021–now**. I also served in the PC of the **ACM Asia Conference on Computer and Communications Security** (ASIACCS) **2023** and the Computer Security track at the **ACM Symposium on Applied Computing** (SEC@SAC) **2019–2022**.
— I have been external **scientific expert** for the ANR (**French National Agency for Research**) Generic Call (ANR main call) in 2019 and in 2020 (both for young researchers and international collaborative research projects).
— I have **co-organized** the GDR Sécurité summer school "Cyber in Nancy 2022".
— I was **co-coordinator** of a joint project between Huawei Technologies Singapore Research Center and ETH Zürich on 5G protocols.
— I am or was a member of the France 2030 ANR PEPR Cybersécurité (SVP) (2022-2026) and ANR Chair IA *ASAP* project (2020-2024). I participated (as external collaborators) to the following funded projects : ERC Consolidator Grant SPOOC, ERC Starting Grant POPSTAR, ANR Chair of research and teaching in artificial intelligence ASAP, ANR project Sequoia, ANR project ProSe, ANR JCJC project VIP.
— I have been external reviewer for the following international conferences : ACM CCS (2020,2017), IEEE CSF (2022,2019,2018), IEEE Euro S&P (2019, 2018), ESORICS (2022,2020, 2019), POST (ETAPS) (2018, 2014), and for the following international journals : ACM Transactions on Privacy and Security (2019, 2022), Journal of Computer Security (2021, 2019, and 2017), IEEE Transactions on Dependable and Secure Computing (2022), IEEE Communications Magazine (2019), and LNCS Transactions on Petri Nets and Other Models of Concurrency (2015).

STUDENT SUPERVISIONS

*PhD students*
*2023-now* — Tom Gouville : DY Fuzzing : Formal Dolev-Yao Models Meet Protocol Fuzz Testing.
*2022-now* — Vincent Diemunsch : Formal Analysis of Industrial Protocols.

*Bachelor and master students*
*2023* — Benjamin Voisin (bachelor (L3) student, ENS de Rennes, France) : ZKP for eligibility verification in e-voting based on OpenID.
— Micol Giacomin (bachelor (L3) student, ENS de Paris-Saclay, France) : Bit-level mutations for DY fuzzers.
— Dominique Bazin (bachelor (L3) student, ENS de Paris, France) : Proving unlinkability based on reachability-based sufficient conditions.
*2021* — Max Ammann (master student at Technical University of Munich, 5 months) : DY fuzzing for testing cryptographic protocols implementations.
*2020* — Guilhem Roy (master student at École Polytechnique ; 5 months) : Symbolic-

Model-Aware Fuzzing of Cryptographic Protocols.

— Timothé Bonhoure (bachelor (L3) student at ENS Lyon ; 2 months) : Improving Cryptographic Protocols Verification : The Best of Two Worlds (co-supervision with Vincent Cheval).

— Karan Agarwalla (bachelor student at IIT Bombay, India ; 2 months) : Formally Comparing and Evaluating Privacy Properties (co-supervision with Steve Kremer).

*2019* — Paul Artigouha (master student at Mines de Nancy ; 1 year, 1.5 days a week) : Formalizing and verifying privacy for the security protocols from the Noise framework.

— Guillaume Girol (master student at ETH Zurich, exchange student from École Polytechnique, France ; 6 months) : Formalizing and verifying the security protocols from the Noise framework (co-supervision with Ralf Sasse). This project resulted in an academic paper published at Usenix Security'20 (see above).

— Silvan Läubli (bachelor (L3) student at ETH Zurich ; 1 year, 1.5 days a week) : Implementing a public bulletin board for Alethea (co-supervision with Lara Schmid).

*2018* — Andris Suter-Dörig (bachelor (L3) student at ETH Zurich ; 1 year, 1.5 days a week) : Formalizing and verifying the security protocols from the Noise framework (co-supervision with Ralf Sasse).

— Vincent Falconieri (master student at ETH Zurich, exchange student from INSA Lyon, France, working as an academic assistant (Hiwi)) : Fuzzing authentication protocols in LTE (co-supervision with Ralf Sasse)

*2017* — Vincent Stettler (master student at ETH Zurich working as an academic assistant (Hiwi)) : NextGen Network Security Analysis (co-supervision with Ralf Sasse). This project eventually resulted in an academic paper published at CCS'18 (see above).

— David Lanzenberger (bachelor (L3) student at ETH Zurich ; 1 year, 1.5 days a week) : Formal Analysis of 5G Protocols (co-supervision with Ralf Sasse).

INDUSTRIAL RELEVANCE & MEDIA COVERAGE

*2023* — In our paper "Reversing, Breaking, and Fixing the French Legislative Election E-Voting Protocol" published at **Usenix'23** and presented at **Real World Cryptography'23**, we analyzed the e-voting protocol used during the 2022 French legislative election, which was the largest political election using e-voting ever in the world. We reversed the protocol, found 6 verifiability and privacy attacks on the protocol, and proposed fixes. We responsibly disclosed our work to the stakeholders, *i.e.,* Europe and Foreign Affairs French Ministry, French National Agency for the Security of Information Systems (ANSSI), and the vendor (Voxaly Docaposte). They have acknowledged our analysis and our attacks and decided to implement our fixes, which now benefit the protocol, that was in particular used to organize three elections in 2023 for three constituencies for which the outcome from 2022 was contested. Our work got some press coverage : l'Est Républicain Inria frontpage, (here and there, in French). We also wrote a vulgarization article article about this and e-voting in general the online newspaper The Conversation (in French).

*2022* — We responsibly disclosed four logical attacks-based vulnerabilities we found with our new Dolev-Yao model-guided fuzzing tool *tlspuffin* that affected the *WolfSSL* TLS library : CVE-2022-42905 (**critical severity**), CVE-2022-42905 and CVE-2022-42905 (**high severity**), and CVE-2022-38153 (medium severity). *wolfSSL* is a lightweight implementation widely used by IoT and embedded devices, and is able to run on OSs and CPUs otherwise not supported.

*2017-2019* — We responsibly disclosed our work *New Privacy Threat on 3G, 4G, and Upcoming 5G AKA Protocols* with the privacy attack we found to the **GSMA consor-**

**tium** of which the most important carriers in the world are members (talks given in 2017 and 2019) as well as to the **3GPP** group, responsible for 3G, 4G, and 5G mobile communication standardization. Since then, we have ongoing discussions with 3GPP and GSMA about potential remedies. We obtained a **formal acknowledgment** of the vulnerability in June 2019, when 3GPP added our attack to the list of the current **key issues** in 5G (see Technical Report 33.846). More recently, various vendors have proposed to 3GPP different Change Requests (CR) with **countermeasures** to fix our attack in 5G : Qualcomm, Gemalto, China Mobile, Thales, Nokia, ZTE, and Huawei. One of those countermeasures made to the official 5G specification (3GPP TS 33.102) as an optional mitigation. Our attack was also presented at **Black Hat USA'17** by a co-author. Our findings got some press coverage : ZDnet 1 and 2, The Register 1 and 2, Forbes, EFF, International Business Times, NextInpact, Silicon.de.

*2018* — We responsibly disclosed the flaws we found with our work *A Formal Analysis of 5G Authentication* to mobile communication standardization bodies (3GPP and GSMA). We still have ongoing discussions with them about potential integration of our countermeasures in the 5G standard; see CVD-2018-0012 from the GSMA Hall of Fame. Our work also got some press coverage : Daily Mail, The National, ACM TechNews, The Hill, SRF 4, Tages-Anzeiger (frontpage), ETHZ news (frontpage), The Courier, 20 Minuten.

*2017* — We investigated and analyzed the insufficient protections afforded to mobile identities when using today's operator-backed WiFi services in our work *Mobile subscriber WiFi privacy*. The privacy attacks we found were acknowledged by device manufacturers (Apple, Google, Microsoft, and Blackberry) and GSMA. As a direct result, **Apple deployed a mitigation in iOS10**.

*2017-2018* — We started mid 2017 a 1 year project (100'000 CHF) between ETH Zürich (David Basin, Ralf Sasse and me) and Huawei Technologies Singapore Research Center whose I was **co-coordinator**. This project involved a bilateral collaboration on NextGen telecommunication security protocols (we analyzed Huawei design proposals, they shared their case studies) and an industrial transfer : Ralf Sasse and I went to Singapore to give a 4 days in-depth tutorial on the (academic) tool Tamarin (automatic prover of formal security guarantees) for a dozen of Huawei engineers. We have thus both promoted formal methods in the industrial sector and made available verification techniques to engineers who will notably be responsible of the standardization and implementation of many security protocols, e.g., in the 5G ecosystem.

TOOLS & SOFTWARE

**tlspuffin** (co-developer) — We developed with Max Ammann (main developer) a fuzzer implementing a novel model-guided kind of fuzzer. The novel idea is to use the security-related domain-specific Dolev-Yao formal model to guide the fuzzer towards finding logical attacks in security protocols. Research conducted with M. Ammann and S. Kremer.
**UKano** (main developer) — Automatic verifier of unlinkability and anonymity for a large class of 2-agents protocols (in OCaml, $\approx$ 2 kloc). Notably used to discover new attacks on ePassport protocols. Open-source, available on Github and at https://projects.lsv.ens-cachan.fr/ukano/.
**Porridge** (co-developer) — Porridge is a standalone OCaml library implementing *Partial Order Reduction* techniques for checking trace equivalence of security protocols. It is not restricted to the limited class of *action-deterministic* protocols as in prior works. It has been successfully integrated into two state-of-the-art verifiers DeepSec and Apte, bringing significant speedups. Webpage at https://members.loria.fr/LHirschi/porridge/index.html with source code and instructions.
**POR for APTE** (main developer) — Implementation of Partial Order Reduction techniques in the tool APTE which considerably improved its practical impact (in OCaml,

$\approx$ 3 kloc). Open-source, available on Github and at http://www.lsv.fr/~hirschi/apte_por. Implementation of similar techniques in the tool SPEC (in Bedwyr, $\approx$ 3.3 kloc).

TEACHING ACTIVITIES

2022 (28h) — Master course on cryptographic protocols at University of Lorraine (responsible and teacher of the course).

(25h) — Applied Mathematics in Comptuer Science at Telecom Nancy (tutorial classes).

2021 (4h) — Invited lecture at the summer school of the GDR IM.

(6h) — Invited lecture at the winter school of the GDR Sécurité.

2020 (32h) — Applied Mathematics in Comptuer Science at Telecom Nancy (tutorial classes).

2019 (32h) — Applied Mathematics in Comptuer Science at Telecom Nancy (mix of lectures and tutorial classes).

2018 (30h) — Computational Science and Engineering at ETH Zürich (back-office TA, design of exams).

(30h) — Information Security at ETH Zürich (head TA, lab classes, and 2 lectures).

2017 (30h) — Numerical Methods for CSE at ETH Zürich (lab classes).

(20h) — Tutorial on the Tamarin prover given at Huawei Technologies Singapore Research Center.

2013-2017 — Teaching assistant at ENS Cachan :

($2*45+12$h) — Computer Programming : C, OCaml, compiler project (lab classes).

($2*22.5$h) — Logic (tutorial classes).

(30h) — Software engineering (project).

($2*11$h) — Introduction to the Coq Proof Assistant (lab classes).

(22.5h) — Projects around Logic : SAT and Coq.

(22.5h) — Computability (tutorial classes).

VISITING & INTERNSHIPS

2016 — 3 month academic visit at University of Oxford with Professor Cas Cremers. The two collaborations started there with respectively Cas Cremers and Ravishankar Borgaonkar resulted in three papers at **PETS'19**, **Euro S&P'19**, and **MoST'17** and a briefing at **Black Hat USA'17**.

2013 — 4 month internship about reduction of interleavings for trace equivalence checking of security protocols with David Baelde & Stéphanie Delaune, LSV, ENS Cachan.

2012 — 3 month internship about infinite and cyclic proofs and Büchi automata directed by David Baelde, PLS lab, IT University of Copenhagen, Denmerk. Work continued later on with Amina Doumane and Alexis Saurin, leading to a publication at **LICS'16**.

— 2 month internship about alternating automata for XPath queries directed by Kim Nguyên, LRI lab, Paris-Sud.

2011 — 6 week internship about type-safe language for XML directed by Giuseppe Castagna and Kim Nguyên, PPS lab, Paris-7.

VULGARIZATION

2023 — Alexandre Debant and myself have written a vulgarization article about e-voting in the online newspasper The Conversation (in French).

2020 — I have co-authored the article *Le traçage anonyme, dangereux oxymore : Analyse de risques à destination des non-spécialistes.* that provides concrete and simple attack scenarios against tracing applications like DP3T or ROBERT, deployed in the context of the covid-19 pandemic, in order point out the necessity to clarify the benefits of such applications so that the general public (and in particular the members of the French parliament) can judge the balance between the benefits and the risks. The publication of this

document was followed by multiple interviews (Le Monde, Les Echos, Le Figaro, Télérama, AEF, France Culture, etc.).
2018-2019 — I have done a couple of interviews with journalists and wrote an ERCIM News article about 5G mobile communication (see above).
2013 — Hosted a one day workshop for secondary school pupils on cryptography at the Science Fair (Fête de la science) 2013.

TECHNICAL SKILLS

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

ADMINISTRATIVE TASKS

I am member of the Association for the management of social works of Inria Nancy (2022-). I was organizing the internal seminar of the Information Security group at ETH Zürich (2018). 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).

*Last modification : 6 décembre 2023*