

Lucca Hirschi

Position: Research Scientist (tenured) at Inria and LORIA, PESTO team, Nancy, France

Email: lucca.hirschi@inria.fr · **Web:** members.loria.fr/LHirschi · [Long CV](#) · [DBLP](#) · [Google Scholar](#) · [GitHub](#)

Research

I develop and apply formal methods to analyze, attack and fix real-world cryptographic protocols, and Dolev-Yao model-guided fuzzing ([puffin](#)) to test their implementations.

Employment and education

2019–now Research Scientist (tenured), Inria, LORIA (Nancy, France). [HDR 2026](#), Université de Lorraine.

2017–18 Postdoc, [Information Security Group of David Basin](#), ETH Zurich, Switzerland.

2017 [PhD](#), ENS Paris-Saclay (S. Delaune, D. Baelde); [best PhD thesis prize](#) of GDR Sécurité.

Awards and grants

2026 [Notable Reviewer'25](#) and [Distinguished Reviewer Award'26](#) at USENIX Security.

2024 [CNIL–Inria Data Protection Award 2023](#) (French legislative e-voting analysis).

2023 [Best Paper Award](#), USENIX Security 2023 (*Hash Gone Bad*).

2022 [PI of the ANR JCJC grant ProtoFuzz](#) (2023–2027, 280 k€).

2017 [Best Paper Award](#), MoST (IEEE S&P Workshops), plus an accepted [Black Hat USA briefing](#).

Selected publications (full list in the [long CV](#))

S&P'27 T. Gouville, L. Hirschi, S. Kremer. *DDYF: Differential Dolev-Yao Fuzzing of Cryptographic Protocols*.

USENIX'25 V. Diemunsch, L. Hirschi, S. Kremer. *A Comprehensive Formal Security Analysis of OPC UA*.

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

USENIX'23 A. Debant, L. Hirschi. *Reversing, Breaking, and Fixing the French Legislative Election E-Voting Protocol*. [CNIL–Inria award](#).

USENIX'23 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*. [Best paper award](#).

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

Supervision, teaching, service and talks

Supervision 4 PhD students, 4 research engineers, 18 master and bachelor interns.

Teaching Responsible for the [M2 course on cryptographic protocols](#), Université de Lorraine; [Inria Academy masterclasses](#) for Trail of Bits, Eviden, Idemia and INSP.

Service PC of USENIX Security (2025–now), ESORICS'24, ASIACCS'23, etc. Scientific expert for the [ANR](#) (2019, 2020) and [VLAIO](#), Flanders (2025). Local member of Inria's ethics committee (COERLE).

Juries President of the [GDR Sécurité PhD artifact award](#) jury; member of the [Gilles Kahn thesis award](#) committee (SIF).

Invited talks [Indocrypt'24](#), [Inria JSI'24](#), [Apple Tech Talks'23](#), [Real World Crypto'23](#), [Troopers'17](#), [GSMA'17](#).

Real-world impact

2024–now [puffin](#). The DY fuzzer I lead found [50+ compliance bugs in 5 TLS and 2 SSH implementations](#), and [5 CVEs in wolfSSL](#) (1 critical, 2 high); used by Trail of Bits for an [OpenSSL audit](#).

2024–25 [OPC UA](#). [8 attacks found by formal analysis](#), acknowledged by the OPC Foundation and filed as [8 GCVEs](#); our provably secure fixes are mostly in the upcoming standard. Presented to the OPC Foundation Security WG with CISA, BSI, ANSSI and the FBI.

2023–25 [French legislative e-voting](#). Reverse-engineered the protocol of the 2022 elections (largest political e-voting election ever) and [found 6 attacks](#); fixes adopted by the [Ministry of Europe and Foreign Affairs](#), ANSSI and the vendor. Consultant to ANSSI for its [e-voting doctrine](#). [CNIL–Inria award](#).

2017–19 [5G](#). [Privacy attack on 3G/4G/5G AKA](#) added to the 3GPP 5G key issues (TR 33.846); a counter-measure made it into the 5G specification (TS 33.102). [GSMA Mobile Security Hall of Fame](#).