Postdoc Position
Dolev-Yao-Model-Guided Fuzzing of Cryptographic Protocols

Duration: 1 to 3 years, starting in 2025 or 2026.

Where: At Inria in Nancy, France. In the Research team PESTO at LORIA. Nancy is a vibrant university city in northeastern France with excellent research facilities and quality of life.

Name and email address of the advisors
Lucca Hirschi, `lucca.hirschi@inria.fr` & Steve Kremer, `steve.kremer@inria.fr`

Salary and Funding: Monthly gross salary from 2 788 € to 3 362 €. This position is already funded by the ProtoFuzz ANR (program managed by the French National Research Agency under grant agreement No. ANR-22-CE48-0017).

TL;DR. We are seeking a post-doctoral researcher to join our puffin [1] team and advance the field of Dolev-Yao model-guided fuzzing of cryptographic protocols (DY fuzzing) [2].

This position offers the opportunity to work on research questions that connect formal verification with practical security testing. Key research directions include:

- exploring e-voting protocol fuzzing applications,
- designing and evaluating novel DY fuzzing building blocks (e.g., feedback metrics, objective oracles),
- partially automating the harnessing and integration of new programs and protocols,
- strengthening the connection between our fuzzing approach and formal methods/symbolic verifiers.

Join us in developing the next generation of security testing tools for cryptographic protocols.

Context. Critical and widely used cryptographic protocols have repeatedly been found to contain flaws in their design and their implementation. A prominent class of such vulnerabilities is logical attacks, e.g., attacks that exploit flawed protocol logic. Automated formal verification methods, based on the Dolev-Yao (DY) attacker, formally define and excel at finding such flaws, but operate only on abstract specification models. Fully automated verification of existing protocol implementations is today still out of reach. This leaves open whether such implementations are secure.

On the opposite side of the spectrum, *fuzz testing*, developed since the 90s, is now the gold standard for testing security software and is used at scale by the largest software companies. However, even if a protocol implementation is tested against memory-related vulnerabilities using state-of-the-art fuzzers, the whole class of *implementation-level logical attacks* remains out of scope. Unfortunately, this blind spot hides numerous attacks, notably recent logical attacks on widely used TLS implementations introduced by implementation bugs.

We have recently addressed this challenge by proposing a novel and effective technique that we called DY model-guided fuzzing [2], which captures logical attacks against protocol implementations. The main idea is to consider as possible test cases the set of abstract DY executions of the formal DY attacker, and use a novel *mutation-based fuzzer* to explore this set. This approach enables reasoning at a more structural and security-related level of messages represented as *formal terms* (e.g., decrypt a message and re-encrypt it with a different key) as opposed to random bit-level modifications that are much less likely to produce relevant logical adversarial behaviors. We have implemented a full-fledged and modular DY protocol fuzzer puffin [1]. We have demonstrated its effectiveness by fuzzing four popular TLS implementations, resulting in the discovery of several novel vulnerabilities, RFC non-compliance errors, and bugs[1]. We are now actively exploring (i) differential fuzzing [7] for DY fuzzing, (ii) using puffin to fuzz ICS protocols such as OPC UA [5], (iii) and combining DY fuzzing with more standard bit-level fuzzing (these are still work-in-progress sub-projects).

This recent work has opened up various exciting new research questions we would like to explore within the puffin team; *i.e.,* Lucca Hirschi (Inria researcher), Steve Kremer (Inria senior researcher), Tom Gouville (PhD student), and Olivier Demangeon (Inria research engineer working on puffin). We would like to hire a post-doc to work with us on research directions related to this project.

[1] Notably CVE-2022-42905 (critical severity), CVE-2022-39173 and CVE-2022-38152 (medium severity).

Potential Research Directions. Depending on the candidate's expertise and interests, we will collaboratively choose among several research directions, such as but not limited to:

1. Explore the application of DY fuzzing to e-voting protocols. Such protocols are critical pieces of software which have not received much attention from the fuzzing community so far. DY fuzzing seems to be ideally placed to address the unique challenges posed by e-voting systems. The protocol and implementation we envision to explore first is the one of SwissPost [6], which is often used in Switzerland. Such a protocol and implementation constitute an interesting target for several reasons: they are based on many different *micro-services* run by different actors and they aim to achieve extremely strong security properties under strong threat models. We also have a strong expertise in e-voting protocols in our team, notably on SwissPost [4].

2. Tighten the link between our fuzzing approach and formal methods and symbolic verifiers which are able to reason about protocols using formal logic. We envision that automated protocol analyzers such as ProVerif or Tamarin [3] could be leveraged to inform the fuzzer on how to synthesize interesting messages, to proxy closeness to attack traces, or to test for privacy properties (which requires deduction capabilities). Another direction is to adapt our framework to test compliance of implementations against a given formal model.

3. Design domain-specific feedback metric to incentivize the fuzzer to seek for new symbolic traces. The underlying fundamental question is: what is a good "symbolic feedback" that promotes semantically different symbolic traces?

4. Define scoring metrics that can be effectively and efficiently computed that can help the fuzzer promoting test cases that are close to attack traces. Using symbolic verifiers to compute such metrics is an option we would like to explore.

5. Design and implement a semi-automatic way to specify the DY model of a protocol (in particular the message model), given as input to tlspuffin. For instance, this could leverage static analysis or code introspection of protocol implementations.

The successful candidate will benefit from dedicated engineering support from our research engineer working on the project, while also being expected to contribute independently to the software development efforts.

Career Development Opportunities. This position offers excellent opportunities for career advancement, including:

- collaboration with leading researchers in formal methods, security, and e-voting,
- participation in international conferences and workshops,
- mentoring opportunities with PhD students and research engineers,
- potential for industrial collaborations and technology transfer.

Required Qualifications and Expectations. We expect mathematical maturity and basic knowledge in logic and theoretical computer science. The ideal candidate should have high expertise in at least one of the following areas: formal methods for cryptographic protocols analysis, fuzzing, or e-voting protocols. In all cases, we require a genuine interest in fuzzing techniques and their applications.

Knowledge in security and cryptography is not mandatory but is definitely a plus. For the implementation work, proficiency in Rust programming is highly desirable.

The successful candidate will be expected to:

- conduct independent research and collaborate effectively within our team,
- publish results in top-tier security and formal methods conferences,
- contribute to the development of our open-source fuzzing framework,
- participate in responsible disclosure of any discovered vulnerabilities.

Salary and Benefits Monthly gross salary from 2 788 € to 3 362 €. Benefits include:

- Subsidized meals
- Partial reimbursement of public transport costs
- Leave: 7 weeks of annual leave + 10 extra days off due to RTT (statutory reduction in working hours) + possibility of exceptional leave (sick children, moving home, etc.)
- Possibility of teleworking (after 6 months of employment) and flexible organization of working hours

- Professional equipment available (videoconferencing, loan of computer equipment, etc.)
- Social, cultural and sports events and activities
- Access to vocational training
- Social security coverage

How to Apply. Interested candidates should send the following documents to both advisors:

- a detailed CV including publication list,
- a cover letter explaining their motivation and relevant experience,
- contact information for 2-3 academic references,
- copies of their most relevant publications (optional but recommended).

References

[1] puffin project. Main webpage: https://tlspuffin.github.io/. Source code: https://github.com/tlspuffin/tlspuffin. Funding: https://project.inria.fr/protofuzz/.

[2] Max Ammann, Lucca Hirschi, and Steve Kremer. DY fuzzing: formal dolev-yao models meet cryptographic protocol fuzz testing. In *Symposium on Security and Privacy*. IEEE, 2024.

[3] Manuel Barbosa, Gilles Barthe, Karthik Bhargavan, Bruno Blanchet, Cas Cremers, Kevin Liao, and Bryan Parno. SoK: Computer-Aided Cryptography. In *Symposium on Security and Privacy (SP)*. IEEE, 2021.

[4] Véronique Cortier, Alexandre Debant, Olivier Esseiva, Pierrick Gaudry, Audhild Høgåsen, and Chiara Spadafora. A practical and fully distributed e-voting protocol for the swiss context. *Cryptology ePrint Archive*, 2025.

[5] Vincent Diemunsch, Lucca Hirschi, and Steve Kremer. A comprehensive formal security analysis of opc ua. In *Usenix Security 2025*, 2025.

[6] Swiss Post. Swiss Post Voting System: System Specification. Version 1.5.0. Technical report, 2025.

[7] Andreas Walz and Axel Sikora. Exploiting dissent: towards fuzzing-based differential black-box testing of tls implementations. *IEEE Transactions on Dependable and Secure Computing*, 2017.