Christof Ferreira Torres

CONTACT INFORMATION

Rua Alves Redol, 9
1000-029 Lisbon
Portugal

GitHub: https://github.com/christoftorres
Email: christof.ferreira.torres@gmail.com
Publications: Google Scholar

RESEARCH INTERESTS

Blockchain, Software Security, Program Analysis, Web Privacy, Fuzz Testing

EDUCATION

University of Luxembourg, Luxembourg, Luxembourg
Technical University of Munich, Munich, Germany
Doctor in Computer Science (Joint Ph.D. - Cotutelle) **April 2018 – May 2022**

- Thesis: *From Smart to Secure Contracts: Automated Security Assessment and Improvement of Ethereum Smart Contracts*
- Graduation Date: *06.05.2022*
- Advisors: *Dr. Radu State* (University of Luxembourg) and *Dr. Claudia Eckert* (Technical University of Munich)

University of Luxembourg, Luxembourg, Luxembourg
Master in Information and Computer Sciences **September 2014 – September 2016**

- GPA: 4.0 (17.5/20.0)
- Thesis: *The Revival of Mining: Anonymised Micropayments via Mined Tickets*
- Advisors: *Dr. Alex Biryukov* and *Dr. Ivan Pustogarov* (Cornell University)

University of Luxembourg, Luxembourg, Luxembourg
Bachelor in Computer Science **September 2011 – July 2014**

- GPA: 3.7 (16.5/20.0)
- Thesis: *Fingerprint Privacy: A Fresh Perspective on Web Privacy*
- Advisors: *Dr. Sjouke Mauw* and *Dr. Hugo Jonker*

PROFESSIONAL EXPERIENCE

Instituto Superior Técnico, University of Lisbon, Lisbon, Portugal **August 2024 – present**
Invited Assistant Professor

- Teaching, research, and supervision of students on various topics related to blockchain security, program analysis, and formal verification in the context of the BIG ERA Chair project.

ETH Zurich, Zurich, Switzerland **August 2022 – July 2024**
Postdoctoral Researcher, Secure & Trustworthy Systems Group (SECTRS)

- Group lead: Dr. Shweta Shinde
- Research on various topics related to trusted computing, blockchain security, program analysis, and formal verification.

University of Luxembourg, Luxembourg, Luxembourg **May 2022 – July 2022**
Postdoctoral Researcher, Services and Data Management Group (SEDAN)

- Group lead: Dr. Radu State
- Research on various topics related to distributed systems, blockchain security and smart contracts.

Luxembourg Tech School, Luxembourg, Luxembourg **September 2018 – July 2020**
Digital Coach

- Teaching basic programming skills in Scratch and Python to high school students between the age of 12 and 18.

Banque et Caisse d'Épargne de l'État, Luxembourg, Luxembourg **April 2018 – March 2022**
PhD Candidate, Software Development Department

- *Blockchain Development and Security Assessment:* Guidance and advice on blockchain security related topics including the security assessment and development of smart contracts.

Fraunhofer AISEC, Garching near Munich, Germany **October 2016 – March 2018**
Research Fellow, Service and Application Security Department

- *Mobile Payment Solution Security Assessment:* Security assessment and penetration testing of mobile payment applications (Android and iOS) with a focus on solutions implementing the Visa

payment standards.

Peer-Reviewed Publications

Conference Papers

1. Analyzing the Impact of Copying-and-Pasting Vulnerable Solidity Code Snippets from Question-and-Answer Websites.
   Konrad Weiss, **Christof Ferreira Torres**, Florian Wendland.
   Proceedings of the 24th ACM Internet Measurement Conference, November 4-6, 2024 **(IMC'24)**.
2. Rolling in the Shadows: Analyzing the Extraction of MEV Across Layer-2 Rollups
   Christof Ferreira Torres, Albin Mamuti, Ben Weintraub, Cristina Nita-Rotaru, Shweta Shinde.
   Proceedings of the 31th ACM Conference on Computer and Communications Security, October 14-18, 2024 **(CCS'24)**.
3. Ethereum's Proposer-Builder Separation: Promises and Realities.
   Lioba Heimbach, Lucianna Kiffer, **Christof Ferreira Torres**, Roger Wattenhofer.
   Proceedings of the 23rd ACM Internet Measurement Conference, October 24-26, 2023 **(IMC'23)**.
4. Is Your Wallet Snitching On You? An Analysis on the Privacy Implications of Web3.
   Christof Ferreira Torres, Fiona Willi, Shweta Shinde.
   Proceedings of the 32nd USENIX Security Symposium, August 9-11, 2023 **(USENIX'23)**.
5. A Ripple for Change: Analysis of Frontrunning in the XRP Ledger.
   Vytautas Tumas, Beltran Borja Fiz Pontiveros, **Christof Ferreira Torres**, Radu State.
   Proceedings of the 5th IEEE International Conference on Blockchain and Cryptocurrency, May 1-5, 2023 **(ICBC'23)**.
6. A Flash(bot) in the Pan: Measuring Maximal Extractable Value in Private Pools.
   Ben Weintraub, **Christof Ferreira Torres**, Cristina Nita-Rotaru, Radu State.
   Proceedings of the 22nd ACM Internet Measurement Conference, October 25-27, 2022 **(IMC'22)**.
7. Elysium: Context-Aware Bytecode-Level Patching to Automatically Heal Vulnerable Smart Contracts.
   Christof Ferreira Torres, Hugo Jonker, Radu State.
   Proceedings of the 25th International Symposium on Research in Attacks, Intrusions and Defenses, October 26-28, 2022 **(RAID'22)**.
8. Frontrunner Jones and the Raiders of the Dark Forest: An Empirical Study of Frontrunning on the Ethereum Blockchain.
   Christof Ferreira Torres, Ramiro Camino, Radu State.
   Proceedings of the 30th USENIX Security Symposium, August 11-13, 2021 **(USENIX'21)**.
9. ConFuzzius: A Data Dependency-Aware Hybrid Fuzzer for Smart Contracts.
   Christof Ferreira Torres, Antonio Ken Iannillo, Arthur Gervais, Radu State.
   Proceedings of the 6th IEEE European Symposium on Security and Privacy, October 7–22, 2021 **(EuroS&P'21)**.
10. The Eye of Horus: Spotting and Analyzing Attacks on Ethereum Smart Contracts.
    Christof Ferreira Torres, Antonio Ken Iannillo, Arthur Gervais, Radu State.
    Proceedings of the 25th International Conference on Financial Cryptography and Data Security, March 1–5, 2021 **(FC'21)**.
11. High-Frequency Trading on Decentralized On-Chain Exchanges.
    Liyi Zhou, Kaihua Qin, **Christof Ferreira Torres**, Duc V Le, Arthur Gervais.
    Proceedings of the 42nd IEEE Symposium on Security and Privacy, May 23-27, 2021 **(S&P'21)**.
12. ÆGIS: Shielding Vulnerable Smart Contracts Against Attacks.
    Christof Ferreira Torres, Mathis Baden, Robert Norvill, Beltran Fiz Pontiveros, Hugo Jonker, Sjouke Mauw.
    Proceedings of the 15th ACM Asia Conference on Computer and Communications Security, October 5–9, 2020 **(AsiaCCS'20)**.
13. A Data Science Approach for Detecting Honeypots in Ethereum.
    Ramiro Camino, **Christof Ferreira Torres**, Mathis Baden, Radu State.
    Proceedings of the 2nd IEEE International Conference on Blockchain and Cryptocurrency, May 2-6, 2020 **(ICBC'20)**.

14. Whispering Botnet Command and Control Instructions.
    Mathis Baden, **Christof Ferreira Torres**, Beltran Borja Fiz Pontiveros, Radu State.
    Proceedings of the 2nd Crypto Valley Conference on Blockchain Technology, June 24-26, 2019 **(CVCBT'19)**.
15. The Art of The Scam: Demystifying Honeypots in Ethereum Smart Contracts.
    Christof Ferreira Torres, Mathis Steichen, Radu State.
    Proceedings of the 28th USENIX Security Symposium, August 14-16, 2019 **(USENIX'19)**.
16. Osiris: Hunting for Integer Bugs in Ethereum Smart Contracts.
    Christof Ferreira Torres, Julian Schütte, Radu State.
    Proceedings of the 34th Annual Computer Security Applications Conference, December 3-7, 2018 **(ACSAC'18)**.
17. Investigating Fingerprinters and Fingerprinting-Alike Behaviour of Android Applications.
    Christof Ferreira Torres, Hugo Jonker.
    Proceedings of the 23rd European Symposium on Research in Computer Security, September 3-7, 2018 **(ESORICS'18)**.
18. The Fréchet/Manhattan Distance and the Trajectory Anonymisation Problem.
    Christof Ferreira Torres, Rolando Trujillo-Rasua.
    Proceedings of the 30th Annual IFIP WG 11.3 Conference, July 18-20, 2016 **(DBSec'16)**.
19. FP-Block: Usable Web Privacy by Controlling Browser Fingerprinting.
    Christof Ferreira Torres, Hugo Jonker, Sjouke Mauw.
    Proceedings of the 20th European Symposium on Research in Computer Security, September 21-25, 2015 **(ESORICS'15)**.

Workshop Papers

1. Revisiting Rollbacks on Smart Contracts in TEE-protected Private Blockchains.
   Chen Chang Lew, **Christof Ferreira Torres**, Shweta Shinde, Marcus Brandenburger.
   Proceedings of the 7th Workshop on System Software for Trusted Execution, July 8, 2024 **(SysTEX'24)**.
2. Timely Identification of Victim Addresses in DeFi Attacks.
   Bahareh Parhizkari, Antonio Ken Iannillo, **Christof Ferreira Torres**, Sebastian Banescu, Joseph Xu, Radu State.
   Proceedings of the 7th International Workshop on Cryptocurrencies and Blockchain Technology, September 28, 2023 **(CBT'23)**.
3. Sluggish Mining: Profiting from the Verifier's Dilemma.
   Beltran Borja Fiz Pontiveros, **Christof Ferreira Torres**, Radu State.
   Proceedings of the 3rd Workshop on Trusted Smart Contracts, February 22, 2019 **(WTSC'19)**.
4. Blockchain for Education: Lifelong Learning Passport.
   Wolfgang Gräther, Sabine Kolvenbach, Rudeolf Ruland, Julian Schütte, **Christof Ferreira Torres**, Florian Wendland.
   Proceedings of the 1st ERCIM Blockchain Workshop, May 8-9, 2018 **(ERCIM'18)**.

Posters

1. ÆGIS: Smart Shielding of Smart Contracts.
   Christof Ferreira Torres, Mathis Baden, Robert Norvill, Hugo Jonker.
   Proceedings of the 26th ACM Conference on Computer and Communications Security, November 11-15, 2019 **(CCS'19)**.

Demos

1. Towards Usable Protection Against Honeypots.
   Christof Ferreira Torres, Mathis Baden, Radu State.
   Proceedings of the 2nd IEEE International Conference on Blockchain and Cryptocurrency, May 2-6, 2020 **(ICBC'20)**.

Awards and Grants

2024 TLDR Research Fellowship (Grant)
Awarded by the Uniswap Foundation to conduct research on cross-chain MEV extraction in the context of Layer-2 shared sequencing. Grant amount: 30,000 USD.

2022 Excellent Doctoral Thesis (Award)
Awarded every year by the doctoral schools of the University of Luxembourg to the best 10% doctoral candidates to acknowledge their outstanding thesis projects.

2022 UBRI Impact (Award)
Awarded by a jury of internationally renowned professors (elected by the Ripple Foundation) as part of the Ripple University Blockchain Research Initiative (UBRI) for outstanding contributions in the field of blockchain research.

2019 Luxembourg's Most Promising Young Talent (Award)
Awarded by the Luxembourgish government for coaching the Luxembourgish national cybersecurity team during the European Cybersecurity Challenge (ECSC) in Bucharest, Romania.

2018 FNR Industrial Fellowship (Grant)
Obtained funding for the entire period of the PhD by the Luxembourgish National Research Fund (FNR) for carrying out research on secure blockchain technologies for the financial sector.

2016 Top Student (Award)
Awarded by the University of Luxembourg as one of the best students of the Faculty of Science, Technology and Communication.

Academic Service

Program Committee (PC) member
ESORICS 2023, FC 2024, DIMVA 2024, ACSAC 2024, NDSS 2025, IEEE S&P 2025, FC 2025, CCS 2025

Technical Program Committee (TPC) member
IEEE ICBC 2019, 2020, 2021, 2022, 2023, 2024, 2025, BLOCKCHAIN 2021, 2022

Journal Reviewer
Elsevier Computers & Security, ACM TOSEM 2022, IEEE TSE 2022, IEEE TIFS 2022

External Reviewer
ESORICS 2019, 2020, ACNS 2021, ISSRE 2021, IEEE EuroS&P 2022, 2023, IEEE S&P 2023

Artifact Evaluation Committee (AEC) member
ACSAC 2022, USENIX Security 2022, 2023, 2024

Teaching Experience

SIRS11 Network and Computer Security
Teaching Assistant (TA), Autumn Semester 2024, Instituto Superior Técnico, University of Lisbon

263-0009-00L Information Security Lab
Head Teaching Assistant (Head TA), Autumn Semester 2023, ETH Zurich

252-4601-00L Current Topics in Information Security
Teaching Assistant (TA), Autumn Semester 2023, ETH Zurich

252-0833-00L Computer Science II
Teaching Assistant (TA), Spring Semester 2023, ETH Zurich

252-1414-00L System Security
Guest Lecture on Smart Contract Security, Autumn Semester 2023, ETH Zurich

252-4601-00L Current Topics in Information Security
Teaching Assistant (TA), Autumn Semester 2022, ETH Zurich

252-0217-00L Computer Systems
Teaching Assistant (TA), Autumn Semester 2022, ETH Zurich

Mentoring

Analysing the Economic Security of Smart Contracts
Master Thesis, Fábio Ribeiro, Instituto Superior Técnico, University of Lisbon, 2024

The Leaky Web3: An Analysis on XSS and XS-Leaks in Web3
Master Thesis, Marino Müller, ETH Zurich, 2024

Defenses against Rollback Attacks for External State Storage
Master Thesis, Chen Chang Lew, ETH Zurich (In collaboration with IBM Zurich), 2023

An Analysis of the Bot Ecosystem on Ethereum
Semester Project, Marino Müller, ETH Zurich, 2023

Detecting Malicious Smart Contract Bytecode Deployments Using Machine Learning
Semester Project, Chunxiao Wu, ETH Zurich, 2023

Resource Exhaustion Attacks on Layer 2
Semester Project, Kaourintin Tamine, ETH Zurich, 2023

Analyzing MEV on Layer-2 Blockchain Rollups
Bachelor Thesis, Albin Mamuti, ETH Zurich, 2023

Fuzzing the WebAssembly System Interface
Bachelor Thesis, Leonhard Koblitz, ETH Zurich, 2022

Data Flow Analysis of EVM Smart Contracts
Master Thesis, Ece Kubilay, Technical University of Munich, 2018

Invited Talks

Exploring the Dark Forest: An Introduction to Maximal Extractable Value (MEV)
- Scientific School on Blockchain & Distributed Ledger Technologies, Cagliari, Italy, September 2024

Rolling in the Shadows: A Closer Look at MEV Extraction Across Layer 2 Rollups
- TUM Blockchain Salon 24, Munich, Germany, May 2024

Is Your Wallet Snitching On You? An Analysis on the Privacy Implications of Web3
- Vienna Cybersecurity and Privacy Research Cluster, TU Vienna, Austria, November 2023
- HOPR Association, Zurich, Switzerland, September 2023
- MIT Digital Currency Initiative, Massachusetts Institute of Technology, Remote, August 2023
- Network and Distributed Systems Security Lab, Northeastern University, Boston, MA, USA, August 2023
- Privacy Innovation Lab, TikTok, Remote, July 2023

Automated Security Assessment of Ethereum Smart Contracts
- International Symposium On Blockchain Advancements, Singapore, December 2022

Property Based Fuzzing with ConFuzzius
- Quantstamp Inc., Remote, August 2022

A Journey on Smart Contract Security: A Story of Glory and Greed
- Secure & Trustworthy Systems Group, ETH Zurich, Switzerland, November 2021

The Art of The Scam: Demystifying Honeypots in Ethereum Smart Contracts
- Ripple UBRI Connect 2019, University of Berkeley, Berkeley, CA, USA, October 2019
- Digital Security Lunch Colloquium, Radboud University, Nijmegen, Netherlands, July 2019

Investigating Fingerprinters and Fingerprinting-alike Behaviour of Android Applications
- Digital Security Lunch Colloquium, Radboud University, Nijmegen, Netherlands, August 2018

Languages

Portuguese: Native Speaker
French: Proficient (C1)
Luxembourgish: Fluent (C2)
English: Fluent (C2)
German: Fluent (C2)
Dutch: Beginner (A1)