

# Erkan Tairi

## Education

- 2019–2024 **PhD in Computer Science**, *TU Wien*, Vienna, Austria  
Supervisors: Matteo Maffei (TU Wien) and Daniel Slamanig (AIT Austrian Institute of Technology)
- 2016–2018 **MSc in Computer Science**, *Johannes Kepler University*, Linz, Austria
- 2011–2015 **BSc in Computer Science**, *University St. Paul the Apostle*, Ohrid, Macedonia

## Professional Experience

- May 2024 - **Postdoctoral Researcher**, *ENS Paris*, Paris, France  
Crypto Team CASCADE  
Host: David Pointcheval
- Mar. 2022 - **Cryptography Consultant**, *MyPrivacy*, Vienna, Austria  
May 2023 Cryptography consultant and software engineer

### Internships and Visits

- Dec. 2022 **Research Visit**, *IMDEA Software Institute*, Madrid, Spain  
Host: Dario Fiore
- Nov. 2022 **Research Visit**, *ETH Zürich*, Zürich, Switzerland  
Host: Dennis Hofheinz
- Jun.-Sep. 2018 **Internship**, *AIT Austrian Institute of Technology*, Vienna, Austria  
Supervisor: Daniel Slamanig
- Oct. 2018 - **Internship**, *TU Wien*, Vienna, Austria  
Mar. 2019 Supervisor: Matteo Maffei

### Teaching

- 2019–2023 **Teaching Assistant**, *TU Wien*, Vienna, Austria  
Cryptocurrencies, Privacy-Enhancing Cryptography (graduate level)

## Publications

### Published Papers

- Lower Bounds for Lattice-based Compact Functional Encryption*. In EUROCRYPT 2024.  
[Erkan Tairi](#) and Akin Ünal
- (Inner-Product) Functional Encryption with Updatable Ciphertexts*. In Journal of Cryptology.  
Valerio Cini, Sebastian Ramacher, Daniel Slamanig, Christoph Striecks and [Erkan Tairi](#)
- LedgerLocks: A Security Framework for Blockchain Protocols Based on Adaptor Signatures*. In ACM CCS 2023.  
[Erkan Tairi](#), Pedro Moreno-Sanchez and Clara Schneidewind
- Foundations of Coin Mixing Services*. In ACM CCS 2022.  
Noemi Glaeser, Matteo Maffei, Giulio Malavolta, Pedro Moreno-Sanchez, [Erkan Tairi](#) and Sri AravindaKrishnan Thyagarajan
- A2L: Anonymous Atomic Locks for Scalability in Payment Channel Hubs*. In IEEE S&P 2021.  
[Erkan Tairi](#), Pedro Moreno-Sanchez and Matteo Maffei

*Post-Quantum Adaptor Signature for Privacy-Preserving Off-Chain Payments.* In FC 2021.  
Erkan Tairi, Pedro Moreno-Sanchez and Matteo Maffei

*Updatable Signatures and Message Authentication Codes.* In PKC 2021.  
Valerio Cini, Sebastian Ramacher, Daniel Slamanig, Christoph Striecks and Erkan Tairi

### Preprints (Under Submission)

*Unbounded Inner Product Functional Encryption from LWE.*  
Valerio Cini and Erkan Tairi

*Ciphertext-Updatable Attribute-based and Predicate Encryption from Lattices.*  
Robert Schädlich, Linda Scheu-Hachtel, Erkan Tairi and Yuejun Wang

*LeOPaRd: Towards Practical Post-Quantum Oblivious PRFs via Interactive Lattice Problems.*  
Muhammed F. Esgin, Ron Steinfeld, Erkan Tairi and Jie Xu

*Towards Verifiable Delay Functions from Non-Parallelizing Languages.*  
Hamza Abusalah, Dario Fiore, Chethan Kamath, Karen Klein and Erkan Tairi

## Professional Activities

### Program Committee

ACM CCS 2025, FC 2025, IACR Communications in Cryptology 2025

### External Reviewer

ACISP 2024; ACM CCS 2021-2023; ACM AFT 2022; ACNS 2024-2025; APKC 2021-2022;  
Asiacrypt 2021, 2024; CANS 2022; Crypto 2023-2024; Eurocrypt 2023, 2025; FC 2021-2024;  
IEEE S&P 2024; IWSEC 2021-2023; ProvSec 2020-2023

### Administration and Organization

- Co-organizer of ViSP Cryptography Research Meetup
- Member of NDSS 2023 Student Support Committee

## Awards and Grants

Erwin Schrödinger Fellowship (by Austrian Science Fund)

## Presentations and Invited Talks

*LedgerLocks: A Security Framework for Blockchain Protocols Based on Adaptor Signatures*  
IOG Seminar. Nov. 2023

*(Inner-Product) Functional Encryption with Updatable Ciphertexts*  
PICOCRYPT Seminar at IMDEA Software Institute. Dec. 2022

*A2L: Anonymous Atomic Locks for Scalability in Payment Channel Hubs*  
IEEE Symposium on Security and Privacy. May 2021

*Post-Quantum Adaptor Signature for Privacy-Preserving Off-Chain Payments*  
Financial Cryptography and Data Security 2021. Mar. 2021  
Decrypto Seminar. Dec. 2020

*Updatable Signatures and Message Authentication Codes*  
Conference PKC 2021. May 2021  
Young Researcher Crypto Seminar. May 2021

## Computer Skills

|             |  |
|-------------|--|
| Programming | C, C++, Rust ( <i>advanced</i> ), C#, Python, Shell ( <i>average</i> ), Java, Go ( <i>basics</i> ) |
| Web         | HTML, CSS, JavaScript (React, Node.js), ASP.NET Web ( <i>advanced</i> )                            |

|          |   |
|----------|---|
| Software | Visual Studio, SageMath, Magma, Git, $\LaTeX$ |
| Other    | Microsoft Azure, Amazon AWS (cloud computing) |

## Languages

|            |        |
|------------|--------|
| Macedonian | Native |
|------------|--------|

|         |        |
|---------|--------|
| English | Fluent |
|---------|--------|

|         |        |
|---------|--------|
| Turkish | Fluent |
|---------|--------|

|        |              |
|--------|--------------|
| French | Intermediate |
|--------|--------------|

|        |              |
|--------|--------------|
| German | Intermediate |
|--------|--------------|

|          |              |
|----------|--------------|
| Albanian | Intermediate |
|----------|--------------|

*professional working proficiency*

*professional working proficiency*

*elementary proficiency*

*elementary proficiency*

*elementary proficiency*

## Referees

|                 |
|-----------------|
| Daniel Slamanig |
|-----------------|

|               |
|---------------|
| Matteo Maffei |
|---------------|

|                  |
|------------------|
| Giulio Malavolta |
|------------------|

|                      |
|----------------------|
| Pedro Moreno-Sanchez |
|----------------------|

*daniel.slamanig@unibw.de*

*matteo.maffei@tuwien.ac.at*

*giulio.malavolta@hotmail.it*

*pedro.moreno@imdea.org*