

Noah Tittelbach

✉ noah.tittelbach@proton.me

Education

ETH Zürich

MSc COMPUTER SCIENCE

Zürich, Switzerland

09.2023-06.2026

- Graduated with distinction
- Grade Average (Swiss Grading Scheme): 6.0; Converted to GPA: 4.0
- Thesis Supervisor: Prof. Dr. Dennis Hofheinz

ETH Zürich

BSc COMPUTER SCIENCE

Zürich, Switzerland

09.2020-09.2023

- Graduated with distinction
- Grade Average (Swiss Grading Scheme): 5.99; Converted to GPA: 4.0
- Thesis Supervisor: Prof. Dr. Ueli Maurer

University of Konstanz

BSc ECONOMICS

Konstanz, Germany

10.2019-09.2020

Ellenrieder Gymnasium

ABITUR

Konstanz, Germany

07.2019

Research Experience

ETH Zürich - D-INFK

SUPERVISORS: PROF. DR. DENNIS HOFHEINZ, DR. EMANUELE GIUNTA

Zürich, Switzerland

Fall 2025

- Master Thesis: "Lower Bounds on Transparent Vector Commitments"
- We prove a lower bound on the size of commitment and openings of algebraic vector commitment (VC) schemes with transparent public parameters (i.e. only uniformly random group elements) in Maurer's Generic Group Model with pairings. We also provide a VC scheme with pairings that beats the lower bound for schemes without pairings, although a gap remains between the construction and the lower bound with pairings.

ETH Zürich - D-INFK

SUPERVISORS: PROF. DR. DAVID BASIN, DR. RALF SASSE

Zürich, Switzerland

Spring 2025

- Research Project: "Modelling Human Errors - in FIDO2"
- Building on a previously created Tamarin model of the FIDO2 protocol, I explored the implications of inexperienced users making errors in the execution of the protocol. This new approach is combined with a redefined model of agent compromise that focuses more clearly on the user's view of the protocol.

ETH Zürich - D-INFK

SUPERVISORS: PROF. DR. KENNETH PATERSON, MATTEO SCARLATA

Zürich, Switzerland

Fall 2024

- Semester Project: "Breaking SSO"
- An analysis of Single-Sign On (SSO) implementations and deployments, focusing on OpenID. We found a pattern of newspaper websites that fail to follow the specification, leading to a vulnerability that allows account hijacking. We also discovered a practical attack against an Identity Provider library based on a JSON format oracle, leading to complete authentication failure.

ETH Zürich - D-INFK

SUPERVISORS: PROF. DR. UELI MAURER, KONSTANTIN GEGIER

Zürich, Switzerland

Spring 2023

- Bachelor Thesis: "Graph-Based Multi-Time Signatures"
- An exploration of digital signature schemes based on one-way/hash functions that can be used to sign a predetermined number of messages k . I proved a lower bound on the size of signatures in relation to k and explored the benefits of allowing each signature to depend on the messages that were signed previously.

Teaching Experience

Fall Terms 2021-2025 Discrete Math, Teaching Assistant

Zürich, Switzerland