Karl Wüst

Dr. Sc. ETH Zurich

Work History

since 01/2023	**Senior Research Scientist**, *Mysten Labs*, Switzerland
10/2021 – 12/2022	**Tenure-Track Faculty (equiv. Assistant Professor)**, *CISPA Helmholtz Center for Information Security*, Saarbrücken, Germany
11/2016 – 09/2021	**Research Assistant & Doctoral Student**, *System Security Group, ETH Zurich*, Zurich, Switzerland
02/2013 – 12/2014	**Student Teaching Assistant**, *ETH Zurich*, Zurich, Switzerland
11/2007 – 04/2013	**Ski Instructor**, *Mountain Adventures AG*, Flims/Laax, Switzerland

Education

11/2016 – 09/2021	**Dr. Sc. ETH Zurich (Computer Science)**, *System Security Group, ETH Zurich*
02/2015 – 07/2016	**MSc in Computer Science**, *Information Security Track, ETH Zurich*
09/2011 – 02/2015	**BSc in Computer Science**, *ETH Zurich*

Publications

[1] **Karl Wüst**, Kari Kostiainen, Noah Delius, and Srdjan Capkun. Platypus: A central bank digital currency with unlinkable transactions and privacy preserving regulation. In *ACM SIGSAC Conference on Computer and Communications Security (CCS)*, 2022.

[2] Srdjan Capkun, Ercan Ozturk, Gene Tsudik, and **Karl Wüst**. ROSEN: RObust and SElective Non-Repudiation (for TLS). In *ACM Cloud Computing Security Workshop*, 2021.

[3] **Karl Wüst**, Loris Diana, Kari Kostiainen, Ghassan Karame, Sinisa Matetic, and Srdjan Capkun. Bitcontracts: Supporting Smart Contracts in Legacy Blockchains. In *Network and Distributed System Security Symposium (NDSS)*, 2021.

[4] **Karl Wüst**, Sinisa Matetic, Silvan Egli, Kari Kostiainen, and Srdjan Capkun. ACE: Asynchronous and Concurrent Execution of Complex Smart Contracts. In *ACM SIGSAC Conference on Computer and Communications Security (CCS)*, 2020.

[5] Sarah Allen, Srdjan Capkun, Ittay Eyal, Giulia Fanti, Bryan A Ford, James Grimmelmann, Ari Juels, Kari Kostiainen, Sarah Meiklejohn, Andrew Miller, Eswar Prasad, **Karl Wüst**, and Fan Zhang. Design choices for central bank digital currency: Policy and technical considerations. Technical report, The Brookings Institution, 2020.

[6] Vasilios Mavroudis, **Karl Wüst**, Aritra Dhar, Kari Kostiainen, and Srdjan Capkun. Snappy: Fast on-chain payments with practical collaterals. In *Network and Distributed System Security Symposium (NDSS)*, 2020.

[7] Sinisa Matetic, **Karl Wüst**, Moritz Schneider, Kari Kostiainen, Ghassan Karame, and Srdjan Capkun. BITE: Bitcoin Lightweight Client Privacy using Trusted Execution. In *28th USENIX Security Symposium*, 2019.

[8] **Karl Wüst**, Kari Kostiainen, Vedran Capkun, and Srdjan Capkun. PRCash: Fast, Private and Regulated Transactions for Digital Currencies. In *International Conference on Financial Cryptography and Data Security*, 2019.

[9] **Karl Wüst**, Sinisa Matetic, Moritz Schneider, Ian Miers, Kari Kostiainen, and Srdjan Capkun.

ZLiTE: Lightweight Clients for Shielded Zcash Transactions using Trusted Execution. In *International Conference on Financial Cryptography and Data Security*, 2019.

[10] Patrick McCorry, Chris Buckland, Surya Bakshi, **Karl Wüst**, and Andrew Miller. You sank my battleship! A case study to evaluate state channels as a scaling solution for cryptocurrencies. In *3rd Workshop on Trusted Smart Contracts*, 2019.

[11] **Karl Wüst** and Arthur Gervais. Do you need a Blockchain? In *2018 Crypto Valley Conference on Blockchain Technology (CVCBT)*, 2018.

[12] Hubert Ritzdorf, **Karl Wüst**, Arthur Gervais, Guillaume Felley, and Srdjan Capkun. TLS-N: Non-repudiation over TLS Enabling Ubiquitous Content Signing. In *Network and Distributed System Security Symposium (NDSS)*, 2018.

[13] **Karl Wüst**, Petar Tsankov, Saša Radomirović, and Mohammad Torabi Dashti. Force Open: Lightweight black box file repair. *Digital Investigation*, 20:S75–S82, 2017.

[14] **Karl Wüst** and Arthur Gervais. Ethereum Eclipse Attacks. Technical report, ETH Zurich, 2016.

[15] Arthur Gervais, Ghassan O Karame, **Karl Wüst**, Vasileios Glykantzis, Hubert Ritzdorf, and Srdjan Capkun. On the Security and Performance of Proof of Work Blockchains. In *ACM SIGSAC Conference on Computer and Communications Security (CCS)*, 2016.

Selected Service & Other Activities

Reviewer (Selection)

Member of the Program Committee for CCS 2023, NDSS 2023 and IEEE ICBC 2019. Reviewer for TIFS (2021, 2022), TDSC (2018). Subreviewer for USENIX Security (2017, 2018, 2019), IEEE S&P (2017, 2018, 2019, 2020, 2021, 2022), CCS (2016, 2018), NDSS (2018, 2019, 2020, 2021, 2022).

Other (Selection)

03/2019 – 02/2021 **Chairman of the Studies Committee**, *ETH Zurich, Department of CS*

01/2018 – 02/2021 **Member of the Studies Committee and the Department Conference**, *ETH Zurich, Department of CS*, Representative of the Scientific Staff

03/2014 – 03/2015 **President**, *Verein der Informatik Studierenden an der ETH Zürich (VIS)*, VIS is the official CS student association at ETH Zurich

11/2014 – 05/2015 **Member of the Selection Committee for Assistant Professorships in Computer Science**, *ETH Zurich, Department of CS*, Student Representative

03/2013 – 09/2014 **Member of the Studies Committee and the Department Conference**, *ETH Zurich, Department of CS*, Student Representative

03/2013 – 03/2014 **Board Member for University Policies**, *Verein der Informatik Studierenden an der ETH Zürich (VIS)*, VIS is the official CS student association at ETH Zurich

Honors and Awards

2022 **ETH Spark Award Top 5 Finalist**
The Spark Award is an award for the best invention at ETH. Nominated for [1].

2020 **ETH Spark Award Top 5 Finalist**
The Spark Award is an award for the best invention at ETH. Nominated for [6].

2016 **Honorary Membership of VIS**
Awarded lifelong honorary membership for extraordinary contributions.

Languages

German	Native
English	Fluent