Jesko Dujmovic

Contact Information

CISPA Helmholtz-Center for Information Security
Stuhlsatzenhausweg 5
66123 Saarbrücken, Germany
Citizenship: German
Email: mail@ind-jesko.net
Website: ind-jesko.net

Current Position

PhD Student
with Nico Döttling
at CISPA Helmholtz-Center for Information Security

Research Interests

My research interests are broadly in theoretical cryptography. Though, I do not shy away from practical work. So far my publications have mostly stuck to communication efficient delegation of computation and restricting cryptographic adversaries in unusual ways. I am currently trying to expand into proof systems and obfuscation.

List of Publications

- **Designated-Verifier SNARGs with One Group Element**
  Gal Arnon, Jesko Dujmovic, Yuval Ishai
  Under Submission
- **Minicrypt PIR for Big Batches**
  Nico Döttling, Jesko Dujmovic, Julian Loss, Maciej Obremski
  Under Submission
- **Registration-Based Encryption in the Plain Model**
  Jesko Dujmovic, Giulio Malavolta, Wei Qi
  PKC 2025
- **Space-Lock Puzzles and Verifiable Space-Hard Functions from Root-Finding in Sparse Polynomials**
  Nico Döttling, Jesko Dujmovic, Antoine Joux
  TCC 2024
- **Lower-Bounds on Public-Key Operations in PIR**
  Jesko Dujmovic, Mohammad Hajiabadi
  Eurocrypt 2024
- **Time-Lock Puzzles with Efficient Batch Solving**
  Jesko Dujmovic, Rachit Garg, Giulio Malavolta
  Eurocrypt 2024

- **Rate-1 Incompressible Encryption from Standard Assumptions**
  Perdo Branco, Nico Döttling, Jesko Dujmovic
  Theory of Cryptography Conference 2022
- **Maliciously Circuit-Private FHE from Information-Theoretic Principles**
  Nico Döttling, Jesko Dujmovic
  Information-Theoretic Cryptography 2022
- **Algebraic Restriction Codes and Their Applications**
  Divesh Aggarwal, Nico Döttling, Jesko Dujmovic, Mohammad Hajiabadi, Giulio Malavolta, Maciej Obremski
  Innovations in Theoretical Computer Science 2022 and *Algorithmica 2023*

Education

- **PhD**
  CISPA and Saarland University, June 2020-expected May 2025
- **B.Sc. and M.Sc.**
  Saarland University, October 2015-May 2020

Teaching

It follows a list of teaching/organizing I've done.

- **Organizer for CISPA Cryptography Seminar**
  CISPA, May 2022 - December 2024
- **Lecturer for Advanced Public-Key Cryptography**
  Saarland University, Winter Semester 2024/2025
- **Teaching Assistant for Quantum Cryptography Seminar**
  Saarland University, Winter Semester 2023/2024
- **Teaching Assistant for Advanced Cryptography Seminar**
  Saarland University, Summer Semester 2023
- **Teaching Assistant for Cryptography**
  Saarland University Summer Semester 2021
- **Organizer for CISPA Bachelor and Master Thesis Colloquium**
  CISPA May 2020 - June 2021
- **Teaching Assistant for Cryptography**
  Saarland University Summer Semester 2020
- **Tutor for Cryptography**
  Saarland University Summer Semester 2019
- **Tutor for Theoretical Computer Science**
  Saarland University Winter Semester 2018/2019
- **Tutor for Concurrent Programming**
  Saarland University Summer Semester 2018
- **Tutor for Theoretical Computer Science**
  Saarland University Winter Semester 2017/2018

Community Service

I've been a subreviewer at these conferences:

- Crypto 2025
- PKC 2025
- ACNS 2025
- Asiacrypt 2024
- Eurocrypt 2024
- Eurocrypt 2023
- Asiacrypt 2023
- Crypto 2023
- TCC 2023
- ICALP 2023
- ACNS 2023
- Crypto 2022
- PKC 2022
- ACNS 2022

Professional Travels

- **Internship with Giulio Malavolta**
  MPI-SP Bochum, June-July 2023
- **Scientific visit with Stefan Dziembowski**
  Warsaw University, August 2022

Talks

I have given the following talks about mine and other people's work:

- **Tiny SNARKs in the Generic Group Model**
  Oberwolfach Cryptography, January 2025
- **Space-Lock Puzzles and Verifiable Space-Hard Functions from Root-Finding in Sparse Polynomials**
  Theory of Cryptography Conference, December 2024
- **Somewhat-Homomorphic Encryption from Sparse LPN and DDH**
  CISPA Cryptography Seminar, November 2024
- **Computational Error Correcting Codes**
  CISPA Cryptography Seminar, October 2024
- **Lower-Bounds on Public-Key Operations in PIR**
  Eurocrypt, May 2024
- **Lower-Bounds on Public-Key Operations in PIR**
  CISPA Cryptography Seminar, March 2024
- **Basics of 2PC**
  CISPA Cryptography Graduate Seminar, October 2023
- **Time-Lock Puzzles with Efficient Batch Solving**
  CISPA Cryptography Seminar, October 2023
- **OT Extensions Cannot Communicate Optimally**
  MPI-SP Bochum, July 2023
- **Simple, Single-Server PIR with Sublinear Server Computation**
  CISPA Cryptography Seminar, April 2023
- **How Not to Use the Random Oracle**
  Young Researchers Cryptography Seminar, March 2023
- **Doubly Efficient Private Information Retrieval**

CISPA Cryptography Seminar, December 2022

- **Rate-1 Incompressible Encryption from Standard Assumptions**
  Theory of Cryptography Conference, November 2022
- **How Not to Use the Random Oracle**
  CISPA Cryptography Seminar, September 2022
- **Maliciously Circuit-Private FHE from Information-Theoretic Principles**
  Information-Theoretic Cryptography, July 2022
- **Post-Quantum Insecurity from LWE**
  CISPA Cryptography Seminar, July 2022
- **Algebraic Restriction Codes and Their Applications**
  Innovations in Theoretical Computer Science, February 2022
- **Maliciously Circuit-Private FHE from Information-Theoretic Principles**
  CISPA Cryptography Seminar, December 2021