ZK from Symmetric Primitives

Carsten Baum, Technical University of Denmark
Peter Scholl, Aarhus University

Abstract:
Zero-Knowledge (ZK) Proofs are cryptographic protocols that allow a prover to show to a verifier that a certain statement is true without giving away any additional information in the process. They are a central tool in modern cryptography, with many interesting and surprising applications. The MPC-in-the-head paradigm (Ishai et al. at SIAM Journal of Computing 2009) is a well-known technique to construct ZK proofs from symmetric assumptions, which yields practical protocols such as ZKBoo (Giacomelli et al. at USENIX Security 2016) or Ligero (Ames et al. at ACM CCS 2017). It has also led to the development of practical post-quantum-secure signature schemes such as Picnic (Chase et al. at ACM CCS 2017).

In our talks, we will give a thorough introduction to the workings of the MPC-in-the-head paradigm. We will also discuss the new VOLE-in-the-head approach (Baum et al. at IACR CRYPTO 2023) to zero-knowledge proofs and show how it can be used to turn the QuickSilver proof system (Yang et al. at ACM CCS 2021) into a digital signature scheme called FAEST (faest.info), and its recent optimizations.

Biography (Carsten Baum):
After obtaining his PhD degree from Aarhus University in 2016, Carsten was a Postdoc at Bar-Ilan University and an Assistant Professor at Aarhus University before joining the Technical University of Denmark in 2022 as Associate Professor. His main research interests lie in multiparty computation, zero-knowledge proofs, and post-quantum cryptographic techniques. As part of this, he recently participated in the DARPA SIEVE program, which led to the FAEST round 1 submission to the NIST call for Additional PQC Digital Signature Schemes. Carsten is also a consultant for Partisia.

Biography (Peter Scholl):
Peter Scholl is an associate professor in the Cryptography & Security group at Aarhus University. He has worked extensively on bringing the theory of secure multi-party computation into practice with more efficient protocols and implementations. In addition, he works on various related technologies such as zero-knowledge proofs, threshold cryptography, homomorphic secret sharing, and post-quantum cryptography. He has been involved in the design of FAEST, a submission to the NIST call for additional post-quantum signature algorithms.