Bocconi

25 JANUARY 2024
11:00 PM

Bocconi University
Room 3-E4-SR03
Via Röntgen 1, Milano (3° floor)

Zero-Knowledge After Prime Time -- Proving Statements Over Z2k

Speaker

Lennart Braun
Phd Student in the cryprtography group
Aahrus University

Abstract

Zero-knowledge proof systems are usually specified for computation over finite fields F2 or Fp for large primes p. On the other hand, all modern CPUs operate on 32 bit or 64 bit integers, which naturally map to rings Z2k. Although Z2k-arithmetic can be emulated using prime moduli, this comes with an unavoidable overhead. Hence, it is desirable to have proof systems natively support computation over Z2k. Constructing and proving efficient and sound protocols for Z2k is however challenging, as many of the cryptographers favorite tools do not work over rings. We have to deal with zero divisors and misbehaving polynomials. This talk focuses on zero-knowledge proofs based on Vector Oblivious Linear Evaluation (VOLE) and the MPC-in-the-Head (MitH) paradigm. We show how to construct efficient VOLE over Z2k based on a variant of Learning Parity with Noise (LPN) and discuss different methods to verify multiplications over Z2k in the VOLE-ZK and MitH settings.

The talk is based on the following papers:

- Appenzeller to Brie: Efficient Zero-Knowledge Proofs for Mixed-Mode Arithmetic and Z2k with Carsten Baum, Alexander Munch-Hansen, Benoit Razet, and Peter Scholl (CCS'21, https://ia.cr/2021/750)
- Mozzarella: Efficient Vector-OLE and Zero-Knowledge Proofs Over Z2k with Carsten Baum, Alexander Munch-Hansen, and Peter Scholl (Crypto'22, https://ia.cr/2022/819)
- ZK-for-Z2K: MPC-in-the-Head Zero-Knowledge Proofs for Z2k with Cyprien Delpech de Saint Guilhem, Robin Jadoul, Emmanuela Orsini, Nigel P. Smart, and Titouan Tanguy (IMACC'23, https://ia.cr/2023/1057)

Università Bocconi
DEPARTMENT OF COMPUTING SCIENCES