FRIEDRICH-ALEXANDER
UNIVERSITÄT
ERLANGEN-NÜRNBERG

TECHNISCHE FAKULTÄT

Informatik-Kolloquium WS 2016/17

Dienstag, 4. Oktober 2016, 14:00 Uhr
Raum 02.134-113
Martensstr. 3, 91058 Erlangen

Russell W.F. Lai
Department of Information Engineering
The Chinese University of Hong Kong

Cryptography for Parallel RAM from Indistinguishability Obfuscation

Since many cryptographic schemes are about performing computation on data, it is important to consider a computation model which captures the prominent features of modern system architecture. Parallel random access machine (PRAM) is such an abstraction which not only models multiprocessor platforms, but also new frameworks supporting massive parallel computation such as MapReduce.
In this work, we explore the feasibility of designing cryptographic solutions for the PRAM model of computation to achieve security while leveraging the power of parallelism and random data access. We demonstrate asymptotically optimal solutions for a wide-range of cryptographic tasks based on indistinguishability obfuscation. In particular, we construct the first publicly verifiable delegation scheme with privacy in the persistent database setting, which allows a client to privately delegate both computation and data to a server with optimal efficiency. Specifically, the server can perform PRAM computation on private data with parallel efficiency preserved (up to poly-logarithmic overhead). Our results also cover succinct randomized encoding, searchable encryption, functional encryption, secure multiparty computation, and indistinguishability obfuscation for PRAM.
We obtain our results in a modular way through a notion of computational-trace indistinguishability obfuscation (CiO), which may be of independent interests.

Kontakt:
Prof. Dr. Dominique Schröder
Lehrstuhl für Informatik 13 (Angewandte Kryptographie)
Fürther Straße 250
90429 Nürnberg