Elektrotechnisches Kolloquium

der Bergischen Universität Wuppertal

Die Fakultät für Elektrotechnik, Informationstechnik und Medientechnik lädt zur Teilnahme an folgender Vortragsveranstaltung mit anschließender Diskussion ein:

Es spricht

Jonas von der Heyden, M.Sc.

Lehrstuhl für IT-Sicherheit und Kryptographie
Prof. Dr.-Ing. Tibor Jager

über das Thema

Towards Advanced Cryptographic Protocols for Real-World Applications

Inhalt:

This thesis aims to facilitate the deployment of advanced cryptographic primitives in the real world.
It does so by designing and implementing post-quantum algorithms on electronic travel documents, and multi-party computation (MPC) on smart meters.
We also introduce a novel pairing-based key-and-message homomorphic encryption (KMHE) scheme for more efficient outsourced MPC.

First, we present PQ-EAC, a post-quantum secure replacement for the Extended Access Control protocol used in electronic machine-readable travel documents (eMRTDs). By substituting Diffie-Hellman key exchange with post-quantum key encapsulation mechanisms, we design eight protocol variants offering different trade-offs between security and efficiency. Our implementation on an ARM SC300 chip demonstrates runtimes of under two seconds at typical data rates, confirming the practical feasibility of migrating eMRTDs to post-quantum security.

Second, we develop the first fully privacy-preserving power flow analysis (PFA) based on MPC. By adopting a Cartesian formulation of Newton's method and exploiting sparsity, we create an efficient MPC implementation that enables smart grid operations without compromising prosumer privacy. Our benchmarks show that for small grids with low network latency, online computation completes in under 30 seconds, demonstrating that MPC-based PFA is practical for preventive smart grid applications.

Third, we present a new KMHE scheme based on bilinear pairings that enables practical rerandomizable garbling schemes (RGS). Our construction reduces garbled gate size by 98.99\% (from 133.43 MB to 1.35 MB) and garbling time by 99.998\% (from 33 minutes to 0.04 seconds) compared to previous BHHO-based approaches. This four-order-of-magnitude improvement makes the SCALES protocol practically feasible for the first time, enabling constant-round outsourced computation secure against adaptive adversaries.

Together, these contributions demonstrate that advanced cryptographic techniques can be made practical through careful protocol design, algorithmic optimization, and implementation strategies tailored to specific application constraints.

T e r m i n: **08.10.2025, 14 Uhr**

O r t: Bergische Universität Wuppertal
Campus Freudenberg, Seminarraum FME 1.04