ICT25-081 - Foundations and Applications of Resource-Restricted Cryptography

Zusammenfassung

Die Kryptographie hat zum Ziel, Daten zu schützen - sei es bei deren Speicherung, Übermittlung, oder Verarbeitung. Um diesem Ziel gerecht zu werden, entwickeln wir Kryptographen Protokolle, welche beweisbare Sicherheitsgarantien erfüllen. "Beweisbar" bedeutet in diesem Zusammenhang, dass wir Angriffe gegen das Protokoll mittels eines mathematischen Beweises ausschließen können, oder zumindest jeglichen Angriff gegen das Protokoll darauf zurückführen können, ein rechnerisches Problem zu lösen, welches die besten Mathematiker trotz intensiver Forschung nicht zu lösen vermögen.

Dieses Projekt befasst sich mit sogenannter Ressourcen-beschränkter Kryptographie (engl. "Resource-Restricted Cryptography", kurz "RRC"). Hier basiert die Sicherheit von Protokollen bewusst auf Problemen, welche in der Praxis zwar zu lösen sind, jedoch eine signifikante Menge an Ressourcen - etwa Rechenleistung, Zeit, oder Speicherplatz - benötigen. RRC ermöglicht Anwendungen, welche mit klassischer Kryptographie (d.h. basierend auf unlösbaren Problemen) nicht realisierbar wären, z.B. Messenger Apps, bei denen Nachrichten abgestritten werden können ("deniable Messaging"), faire verteilte Berechnungen ("fair multi-party Computation"), oder Blockchain-Technologien. Ziel dieses Projektes ist es, neue Anwendungen insbesondere im Bereich Privacy zu finden, neue kryptographische Primitive zu entwickeln, sowie die Grundlagen von RRC zu erforschen.

Wissenschaftliche Disziplinen:
Cryptology (60%) | IT security (30%) | Theoretical computer science (10%)

Keywords:
privacycryptographyprovable security

Principal Investigator:	Karen Azari (Formerly Klein)
Institution:	University of Vienna
Co-Principal Investigator(s):	Krzysztof Pietrzak (Institute of Science and Technology Austria (IST Austria)) Dominique Schröder (TU Wien)

Status: Laufend (01.10.2026 - 30.09.2030)
GrantID: 10.47379/ICT25081

Weiterführende Links zu den beteiligten Personen und zum Projekt finden Sie unter

https://www.gmbh.wwtf.at/funding/programmes/ict/ICT25-081/