ICT25-075 - Cross-Domain Privacy-Preserving Protocols and Symmetric Cryptography

Zusammenfassung

Das CrossPings-Projekt zielt darauf ab, die Sicherheit und den Datenschutz von Internet-of-Things (IoT)-Geräten zu verbessern – also von Milliarden kleiner, vernetzter Geräte in Smart Homes, im Gesundheitswesen, in Fabriken und anderen Bereichen. Da die Zahl der IoT-Geräte bis 2030 fast 39 Milliarden erreichen wird, ist der Schutz ihrer Daten und Abläufe entscheidend.

Die heutige IoT-Sicherheit beruht auf leichtgewichtiger Kryptographie, die für Geräte mit begrenzter Rechenleistung und Speicher entwickelt wurde. Im Gegensatz dazu sind moderne datenschutzfreundliche Verfahren wie Zero-Knowledge Proofs (ZKP) und Multi-Party Computation (MPC) für leistungsstarke Computersysteme mit weit mehr Ressourcen ausgelegt. CrossPings will diese Welten verbinden, indem neue kryptographische Verfahren entstehen, die sowohl effizient als auch datenschutzfreundlich sind.

Das Projekt wird:

- Sichere und effiziente kryptographische Werkzeuge (z. B. Hashfunktionen, Blockchiffren) für datenschutzfreundliche Berechnungen auf IoT-Geräten entwickeln.

- Datenschutzwahrende Operationen wie Geräteauthentifizierung und sichere Datenverarbeitung ermöglichen.

- Ein formales Sicherheitsrahmenwerk für IoT-Cloud- und Blockchain-Anwendungen schaffen.

CrossPings baut auf der Forschung von E. Andreeva, G. Fuchsbauer und A. Roy auf, die gemeinsam praxisnahe, leichtgewichtige und arithmetisierungsorientierte Algorithmen für sichere IoT-Anwendungen mit MPC- und ZKP-Protokollen entwickeln.

Wissenschaftliche Disziplinen:
Cryptology (100%)

Keywords:
Privacy for IoT and Cloud Privacy-Preserving Blockchains for IoTZero-knowledge proofsMulti-party computationAuthenticated EncryptionBlock CiphersHash functionsProvable securityCryptanalysis

Principal Investigator:	Elena Andreeva
Institution:	TU Wien
Co-Principal Investigator(s):	Arnab Roy (Universität Innsbruck) Georg Fuchsbauer (TU Wien)

Status: Laufend (01.01.2026 - 31.12.2029)
GrantID: 10.47379/ICT25075

Weiterführende Links zu den beteiligten Personen und zum Projekt finden Sie unter
https://wwtf.at/funding/programmes/ict/ICT25-075/