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

Abstract

A large part of cryptography today is tailored for technology domains such as the Internet of Things (IoT), privacy-preserving (PP) computation in the Cloud or cryptocurrencies. Cross-domain security solutions for Privacy-in-IoT, Privacy-Preserving-Blockchains-for-IoT and Privacy-Preserving-IoT-to-Cloud-Computation can enable private IoT identification and payments, and computation on encrypted IoT data via modern cryptographic protocols like zero-knowledge proofs (ZKP) and multi-party computation (MPC). A main obstacle for such cross-domain applications lies in the design gaps for the available symmetric cryptography: while in IoT, the cryptography has to be resource-constrained, lightweight (LW), bit-oriented and aims classical security, in MPC and ZKP it is computationally heavy, integer-based or arithmetization-oriented (AO), and satisfies the protocol security targets.

In this project we will develop secure symmetric-key cryptographic solutions that empower the synergy of LW with ZKP, and LW with MPC. We will identfy target use-cases, formalize and adapt the suitable formal privacy-friendly frameworks, analyze and protect against the relevant cross-domain threats (including side-channel attacks), build (design and analyse) the supporting symmetric-key cryptography consisting of hash functions, ciphers, modes, and implement those. Some of the most important CrossPings project ideas stem from works of the three PIs: Eevee for IoT-to-Cloud [CCS23] and ForkAE LW [ASIACRYPT19] by Andreeva, MiMC [ASIACRYPT16], Poseidon [USENIX21] by Roy, ABR [EUROCRYPT21] and ELC-PGV [CSF24] AO designs by Andreeva and Roy, cryptanalysis [EUROCRYPR24,SAC24,SAC20] by Roy and ZKP protocols [CRYPTO18,ASIACRYPT22,EUROCRYPT24] by Fuchsbauer. We will deliver the first practical symmetric-key algorithms under the best-suited MPC or ZKP protocols for cross-domain use.

Scientific disciplines:
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: Ongoing (01.01.2026 - 31.12.2029)
GrantID: 10.47379/ICT25075

Further links to the persons involved and to the project can be found under
https://www.gmbh.wwtf.at/funding/programmes/ict/ICT25-075/