General information

NXP Semiconductors

Miroslav Knezevic
miroslav.knezevic@nxp.com

Florian Boehl
florian.boehl@nxp.com

Ilya Kizhvatov
ilya.kizhvatov@nxp.com

Area of interest	**Interested**
○ Functional encryption and reduction of leakage (e.g., anonymization or obfuscation)	*Y*
○ Ultra-lightweight cryptology and ultra-high-speed cryptographic algorithms including quantum cryptography	**Y**
○ Physical cryptanalysis, including tampering, side channel, faults injection attacks, and security of tools for good software implementation and validation practices	**Y**
○ Authenticated encrypted token research for mobile payment solution	*Y*
○ Innovative cryptographic primitives and complementary non-cryptographic privacy-preserving mechanisms to enforce privacy	**Y**
○ New techniques, such as quantum safe cryptography, which are secure from quantum computers	**Y**
○ Quantum key distribution	N
○ Automated proof techniques for cryptographic protocols	*Y*
Y = definitely interested / *Y* = depends on direction of proposal / N = rather not interested	

Competencies

- *NXP's Innovation Center for Crypto & Security employs > 120 security experts; focus areas include*
  - **physical security (leakage resilience, fault attacks, tamper resistance),**
  - **(ultra-)lightweight cryptography (PRINCE cipher),**
  - **privacy-preserving mechanisms for constrained hardware (VCA) and**
  - **post-quantum cryptography.**
- *NXP is currently participating in H2020 projects PQCrypto, HEAT, ECRYPT-NET (2 PhD students)*
- *Besides strong expertise in the focus areas above NXP can offer*
  - **insights in current practical constraints for cryptographic solutions on embedded devices and**
  - **an advanced lab environment with bespoke equipment for fault and side-channel attacks and analysis.**