securityandtrust.lu

UNIVERSITÉ DU LUXEMBOURG

General information

SnT, APSIA group, University of Luxembourg
Peter B. Roenne
peter.roenne@uni.lu
+352 466644 5079

Area of interest	Choose Y or N
○ 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	N
○ 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**	**Y**
○ Automated proof techniques for cryptographic protocols	Y

SnT securityandtrust.lu

uni.lu UNIVERSITÉ DU LUXEMBOURG

Competencies

- *Broad knowledge and experience in cryptography at expert level*
- *Experience from other European projects*

Project idea

Quantum Key Distribution (QKD)

- *Novel protocols*
  - **Security against stronger adversaries**
  - **Deniability**
  - **Coercion-resistance**
  - **Embedding in standard crypto, e.g. PKI, for enhanced properties**
  - **Authentication protocols, Q-AKEs**
  - **Fairness in Quantum Protocols**

- *List of the complementary skills you need for your consortium*
  - **Partners especially with knowledge on experimentation and validation**