General information

KU Leuven - iMinds - COSIC

Dave Singelée (research manager)

Dave.Singelee@esat.kuleuven.be

www.esat.kuleuven.be/cosic

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	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	N

KU LEUVEN

iMinds
CONNECT.INNOVATE.CREATE

Competencies

- *Electrical Engineering department @ KU Leuven*
- *5 professors, +/- 70 researchers*
- *Head of the group: prof. Bart Preneel*

- *Participation in over 45 European research projects (9 as coordinator)*
- *Currently 7 ongoing H2020 projects*

- *Strong expertise in*
  - **Cryptography**
  - **Privacy-enabling technologies**
  - **Embedded Security**
- *Research Interests*
  - **Lightweight cryptography, post-quantum crypto, authenticated encryption, PETs, Secure Multi-Party Computation, side-channel and fault injection attacks, HW roots of trust, etc.**