General information

MIRACL.com

Mike Scott

Mike.scott@miracl.com

+353 86 3888746

Area of interest	Choose Y or N
○ Functional encryption and reduction of leakage (e.g., anonymization or obfuscation)	N
○ 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	N
○ 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

Competencies

- *Pairing based Crypto and Authentication*
- *Previous involvement in EU projects and proposals*
- *Elliptic Curve/Pairing-Based Crypto skills, efficient implementations*