

# General information

*Thales UK, Research and Technology*

*Adrian Waller*

[adrian.waller@uk.thalesgroup.com](mailto:adrian.waller@uk.thalesgroup.com)

*+44 (0)118 923 8304*

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	N
○ Automated proof techniques for cryptographic protocols	Y

# Competencies

- *Organisation competencies*
  - **Implementation of cryptographic algorithms and devices (Hardware Security Modules (HSM)s, Key Managers, Network/Link layer Secure Communications,...)**
  - **Application of cryptography in real-world scenarios (practical constraints, system architectures, security management, ...)**
- *Organisation experience in the European project*
  - **Extensive across many technology and application areas. In cryptography, current projects include:**
  - **EC H2020 SAFEcrypto (“Quantum Safe” cryptography) – WP Leader, Standards Liaison Manager**
  - **EC H2020 HEAT (Homomorphic Encryption) – WP Leader**
- *The skills you can bring*
  - **Knowledge of implementation techniques, technologies, constraints, assurance, etc.**
  - **Use cases from across the Thales Group (Aerospace, Security, Transport (Road/Rail/Maritime), Space,...)**

## Project idea

- *Describe your project idea*
- *List of the complementary skills you need for your consortium*