UNIVERSITY OF CAMBRIDGE

General information

University of Cambridge, Centre for Photonic Systems
Adrian Wonfor, Richard Penty
aw300@cam.ac.uk , rvp11@cam.ac.uk
+44 1223 748355, +44 1223 748358

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	N
○ Physical cryptanalysis, including tampering, side channel, faults injection attacks, and security of tools for good software implementation and validation practices	N
○ Authenticated encrypted token research for mobile payment solution	N
○ 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	Y
○ Automated proof techniques for cryptographic protocols	N

UNIVERSITY OF CAMBRIDGE

Competencies

- *Extensive expertise in telecommunications and datacommunications*
- *Photonic Integration for optical sources and switches etc.*
- *Partner UK Quantum Communications Hub*

- *Many EU projects for photonic integration, communications (PONs Long Haul telecoms etc.) Energy efficient communications*

- *Test-beds and demonstrators for combination of QKD with encrypted conventional traffic*
- *Cambridge Quantum Network demonstrator (QKD and high data-rate (Multiple 100Gb/s) telecoms flexible topology network within Cambridge).*
- *Partner in UK national dark fibre network NDFIS (QKD compatible)*
- *Dedicated QKD enabled link to BT labs Adastral Park*

UNIVERSITY OF CAMBRIDGE

Site for QKD test-beds

- *Large QKD compatible test-beds.*
- *Within Cambridge (30km), to BT (150km), UK Dark Fibre Network (500km)*

- *Experimental group with extensive communications experience, with 100Gb/s transmission systems and QKD equipment from major vendors (ID Quantique and Toshiba)*