Finanziato dall'Unione europea
NextGenerationEU

Ministero dell'Università e della Ricerca

Italiadomani
PIANO NAZIONALE DI RIPRESA E RESILIENZA

ROME TECHNOPOLE
INNOVATION ECOSYSTEM

Development and applications of quantum-resistant encryption algorithms, also in the functional encryption environment

Spoke 1	
Task	1.1 Fundamental Research
FP 5	Digital transition through AESA (Active Electronically Scanned Array) radar technology, quantum cryptography and quantum communications
Thematic line	Digital Transition
Workgroup	Antonio Corbo Esposito
Additional human resources	RTDa, Rosa Fera (PhD)
Objective	Quantum computers threaten many of the currently known cryptographic algorithms. Therefore, it is essential to propose new algorithms that are resistant to such attacks. In particular, multivariate cryptography is based on a mathematical problem that is difficult to solve and its study and investigation can lead to a valid encryption and/or digital signature scheme.
Use case / Field of potential application	/
Starting TRL	1
Final TRL	2
Collaborations	Università degli Studi di Napoli Federico II, Università degli Studi di Trento