UNIONE EUROPEA
Fondo Sociale Europeo
Fondo Europeo di Sviluppo Regionale

Ministero dell'Università e della Ricerca

PON RICERCA E INNOVAZIONE 2014 - 2020

Consiglio Nazionale delle Ricerche

Sviluppo di sistemi e tecnologie quantistiche per la sicurezza informatica in reti di comunicazione QUANCOM

L'estensione della rete IP, lo sviluppo ulteriore delle sue applicazioni verso una società sempre più inclusiva (v. la nascita di Internet of Things e nuova generazione di rete wireless 5G) e verso un nuovo modo di produrre (v. la manifattura Industria 4.0) sono sempre di più condizionati dal livello di sicurezza che si riesce a garantire alla rete stessa. Oggi questa sicurezza non si può dire essere "incondizionata", cioè inattaccabile anche con illimitate capacità di calcolo. Le tecnologie di sicurezza sia negli strati trasmissivi della rete che in quelli applicativi stanno diventando sempre più complesse ma ugualmente non sono completamente immuni da attacchi. Infatti aumenta di pari anche la potenza di calcolo, (parallela e distribuita proprio grazie alla potenza della rete) a disposizione delle organizzazioni che per diversi scopi hanno interesse ad appropriarsi di dati sensibili in rete.

Il Progetto QUANCOM si propone di superare radicalmente questa impasse fra attaccante e difesa proponendo un'azione coordinata per lo sviluppo e la sperimentazione di protezione incondizionata della rete IP che ha al suo nucleo la criptografia quantistica. Essa, introdotta per la prima volta nel 1984 e da allora sperimentata con successo in numerose occasioni, è intrinsecamente sicura e capace di resistere a qualsiasi attacco: si basa sulla trasmissione ottica di quantum-bit e sulla trasmissione inattaccabile di chiavi fra trasmettitore e ricevitore (Quantum Key Distribution QKD) Dopo più di 30 anni di sperimentazione in laboratorio, ci sono oggi condizioni per realizzare e sperimentare in campo (per la prima volta) una rete

ottica QKD e di integrare la chiave criptata così trasmessa con altri strati di sicurezza convenzionale per la protezione del traffico sensibile IP. La sperimentazione avverrà su di una rete ottica passiva di tipo metropolitano installata in una grande città del sud Italia.
Accanto a questo primo obiettivo realizzativo (limitato per ragioni tecnologiche al solo ambito metropolitano) il Progetto prevede anche l'esplorazione di altri due temi strategici che permetteranno in futuro di estendere la stessa tecnica in ambiti intra-metropolitani, e quindi all'intera dorsale IP: lo sviluppo ed il completamento della rete in fibra per la trasmissione del segnale di tempo sicuro quale base di test QKD; la sperimentazione di sistemi ibridi di comunicazione optical fiber-free space" come base per lo sviluppo di applicazioni QKD in ambito spaziale.

Il partenariato del progetto Quancom è cosi organizzato: **CONSIGLIO NAZIONALE DELLE RICERCHE (CNR) COORDINATORE, Agenzia Spaziale Italiana, Università di Padova, INRIM, EXPRIVA Spa, Memory Consult srl, DEMETRIX srl**

Il progetto è cofinanziato dal MUR **PON Ricerca e Innovazione 2014-2020**, Decreto Direttoriale di concessione dell'agevolazione del 26/03/2021 prot. n. 728, Codice MIUR ARS01_00734 con un costo totale di € 9.225.000 ed un finanziamento MUR pari a € 4.276.763,72,

QUANCOM è strutturato in 5 Obiettivi Realizzativi

Il progetto è coordinato dal Dipartimento di scienze fisiche e tecnologie della materia del CNR sotto la responsabilità scientifica del prof. Giovanni Piero Pepe – Professore Ordinario dell'Università di Napoli *Federico II* ed Associato CNR- SPIN (Istituto che volge la funzione di capofila).

CNR-SPIN partecipa alle attività di progetto specifiche con riferimento agli OR 4 e OR5 in particolare:

Att 4.1: Individuazione parametri dei dispositivi a singolo fotone

Att 4.3: Sorgenti ottiche non-classiche

Att 4.4: Sistemi di rivelazione per QKD

Att. 5.1: Sviluppo di sistema di QKD punto-punto per connessioni in fibra e free-space

Att.5.4: Sviluppo di un dimostratore QKD per lo scambio di chiave satellite-terra