FONDAZIONE LINKS CAPOFILA NELLA CYBERSICUREZZA QUANTISTICA
CINQUE MILIONI DA BRUXELLES PER UN CONSORZIO A TRAZIONE TORINESE

In tre anni undici partner di quattro Paesi dovranno definire i processi necessari a difendere dati e processi dalla potenza di calcolo illimitata dei nuovi computer. Il progetto QuBip è stato selezionato tra undici proposte arrivate a livello europeo

Torino, 12 settembre 2023

Fondazione Links, ente strumentale della Fondazione Compagnia di San Paolo e del Politecnico di Torino, rafforza il suo ruolo nel settore della cybersecurity traguardando la rivoluzione del quantum computing. Links in qualità di capofila di un consorzio internazionale composto da enti di ricerca, accademie e partner industriali ha ottenuto un finanziamento triennale di cinque milioni di euro dalla Commissione Europea per il progetto QuBip per sviluppare sistemi di cybersicurezza in grado di resistere alla potenza di calcolo di questi nuovi computer.

"*Gli algoritmi di crittografia sono il fondamento della sicurezza della rete Internet e delle applicazioni Internet, come ad esempio i pagamenti on line, home banking, la firma digitale e l'autenticazione dei siti web. Per rompere gli algoritmi crittografici oggi in uso, anche con la massima potenza di calcolo oggi disponibile, servirebbero degli anni. A un computer quantistico basteranno pochi secondi*" spiega Andrea Vesco, a capo della ricerca sulla cybersecurity di Fondazione Links. "*Partendo dai nuovi algoritmi crittografici a chiave pubblica che si stanno sviluppando per "difendere" i dati dalla potenza di calcolo di questi nuovo computer, il nostro obiettivo è definire un processo di transizione degli attuali protocolli di comunicazione e dei sistemi che sia replicabile e di riferimento, che inoltre possa essere utilizzato in maniera standard, una sorta di strada maestra* - spiega ancora Vesco- *ecco perché ci concentreremo su tre esercizi concreti: navigare su internet utilizzando i protocolli resistenti agli attacchi del computer quantistico; come riprogettare l'hardware dell'Industria 4.0; mettere in sicurezza i sistemi degli operatori telefonici della rete 5G*".

"*Il progetto ha preso avvio nei laboratori di Fondazione Links oggi con il kick off meeting. Per noi rappresenta certamente un punto d'orgoglio. L'avvento del computer quantistico è una certezza che possiamo collocare tra 10-15 anni, anche visti gli attuali rate di finanziamento della ricerca industriale in questo settore*" sottolinea Stefano Buscaglia, direttore di Fondazione Links. "*Tra le altre IBM e Google, hanno già attivato due di questi computer quantistici, e in un caso si è già superata la potenza di calcolo di oltre 400 Quantum Bit (QuBit)* - aggiunge – *noi con un altro gruppo di lavoro abbiamo avviato importanti collaborazioni con il centro ricerca della Nato a La Spezia e altri soggetti, tra cui il Politecnico, protagonisti di questa transizione. Per Torino potrebbe rivelarsi un vantaggio strategico nel medio e lungo termine*".

Il computer quantistico, infatti, con la sua straordinaria capacità computazionale permetterà di ottenere nuove scoperte e importanti risultati in tutti i settori scientifici e tecnologici. Allo stesso tempo però, sarà anche in grado di rompere la crittografia a chiave pubblica utilizzata per la sicurezza di tutti i servizi digitali sulla rete Internet. Dalle banche online ai pagamenti alle comunicazioni private, dai controlli dei sistemi delle infrastrutture critiche nazionali fino a quelle di sicurezza. "*Ciò richiede di ridisegnare, riscrivere e ripensare i protocolli dei sistemi di comunicazione per la rete Internet già ora, con l'obiettivo di trovare con largo anticipo, soluzioni adatte ai sistemi più avanzati ma anche a quelli più semplici ma più diffusi, utilizzati da miliardi di persone tutti i giorni. Dall'identità digitale per*

accedere ai comuni servizi informatici alla firma digitale dei documenti, tutte le protezioni possono essere eluse in pochi istanti da calcolatori con queste potenze" spiega ancora Vesco. Di qui la necessità di creare soluzioni crittografiche resistenti agli attacchi del computer quantistico di nuova generazione, su cui lavora la comunità globale dei crittografi in centri ricerca privati e pubblici, coordinati dal Nist (National Institute of Standard and Technology) che in 7 anni ha lanciato ben 4 call per la creazione di nuove soluzioni crittografiche.

QuBip affronta invece un problema più ingegneristico che crittografico, ovvero modificare gli attuali protocolli e sistemi per utilizzare queste nuove soluzioni crittografiche. Il progetto europeo Qubip è tra i primi due progetti finanziati dalla Commissione Europea sul tema della transizione alla crittografia post-quantum dei protocolli internet e dei sistemi connessi. Il progetto ha ricevuto un finanziamento totale di 5 milioni di euro ed è coordinato da Fondazione Links, e vede la collaborazione in tutto di 11 partner di alto livello scientifico da 4 Paesi europei (Italia, Spagna, Finlandia e Repubblica Ceca). Ne fanno parte: gruppi di enti di ricerca (Links, Csic), enti accademici (Politecnico di Torino, Università di Tampere, Universidad Politécnica de Madrid), nonché partner industriali (Red Hat, Security Pattern, Telsy, Telefónica) e utenti finali (Ciber Voluntarios, Smart Factory).

La varietà dei partecipanti al consorzio è legata alla natura del problema da affrontare, che è multidisciplinare, ecco perché al progetto partecipano enti e soggetti di varie origini dai centri ricerca nelle tlc digitali, matematici e utilizzatori finali. Parallelamente a questo progetto, è stato anche finanziato un secondo consorzio, il PQ-React, che invece lavora a portare tra le altre nelle blockchain queste crittografie. Il team di Links, cui sarà destinato circa il 10% del budget complessivo, ha tre anni per definire il nuovo processo di transizione replicabile e di riferimento. "*Il nostro lavoro avrà un impatto anche per i produttori di device, dai computer agli smartphone, di conseguenza sull'utilizzatore finale*" sottolinea Buscaglia.

Ufficio stampa Fondazione Links
Roberto Veronesi
roberto.veronesi@linksfoundation.com
Jan Pellissier
347 7845273