Settimanale
18-09-2023
Pagina 6
Foglio 1 / 2

Fondazione Compagnia di San Paolo

CORRIERE TORINO L'Economia NORD OVEST

www.ecostampa.it

Super computer, a Torino la ricerca sulla cybersecurity

Fondazione Links ottiene 5 milioni di finanziamenti da Bruxelles

Un finanziamento triennale da 5 milioni di euro forniti dalla Commissione Europea per portare avanti il progetto «QuBip», sviluppando sistemi di cybersicurezza in grado di resistere alla potenza di calcolo dei computer quantistici del futuro. È questo il risultato raggiunto da Fondazione Links, ente strumentale della Fondazione Compagnia di San Paolo e del Politecnico di Torino, che rafforza così il proprio ruolo a livello internazionale essendo capofila di un progetto che vede coinvolti altri 10 partner di alto livello scientifico di 4 Paesi europei (Italia, Spagna, Finlandia e Repubblica Ceca).

«Gli algoritmi di crittografia sono il fondamento della sicurezza della rete Internet e delle sue applicazioni — spiega Andrea Vesco, a capo della ricerca sulla cybersecurity di Fondazione Links — come i pagamenti online e la firma digitale. Per rompere gli algoritmi crittografici oggi, anche con la massima potenza di calcolo disponibile, servirebbero anni. A un computer quantistico, invece, basteranno pochi secondi». E proprio qui entra in gioco il progetto «QuBip», pronto a sviluppare sistemi per utilizzare le nuove soluzioni crittografiche e proteggere gli utenti dai computer del futuro. L'obiettivo è definire un processo di transizione degli attuali protocolli di comunicazione che sia replicabile e di riferimento, da usare in maniera standard, una sorta di strada maestra. «Ci concentreremo su tre esercizi concreti — riprende Vesco — dalla classica navigazione sul web alla riprogettazione dell'hardware dell'industria 4.0, fino ad arrivare ai sistemi degli operatori telefonici della rete 5G».

Il computer quantistico, infatti, se da una parte permetterà di ottenere importanti risultati in tutti i settori scientifici e tecnologici, dall'altra rischia di rompere qualsiasi sistema di sicurezza. Dalle banche online alle infrastrutture nazionali. Quando? «Tra 10, o al massimo 15 anni — aggiunge Stefano Buscaglia, direttore di Fondazione Links—. 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».

Per questo «diventa indispensabile ridisegnare, riscrivere e ripensare i protocolli dei sistemi di comunicazione per la rete Internet già ora — aggiunge Vesco—. Dobbiamo trovare con largo anticipo soluzioni adatte ai sistemi più avanzati ma anche a quelli più semplici e diffusi, utilizzati da miliardi di persone tutti i giorni. Dall'identità digitale per accedere ai servizi informatici alla firma digitale dei documenti: tutte le protezioni possono essere eluse in pochi istanti da calcolatori con queste potenze». Un problema su cui sta lavorando, da ben 7 anni, la comunità globale dei crittografi, coordinati dal National Institute of Standard and Technology.

Nicolò Fagone La Zita

Il progetto
Sviluppare sistemi e protocolli in grado di proteggersi dai computer del futuro


Super computer, a Torino la ricerca sulla cybersecurity

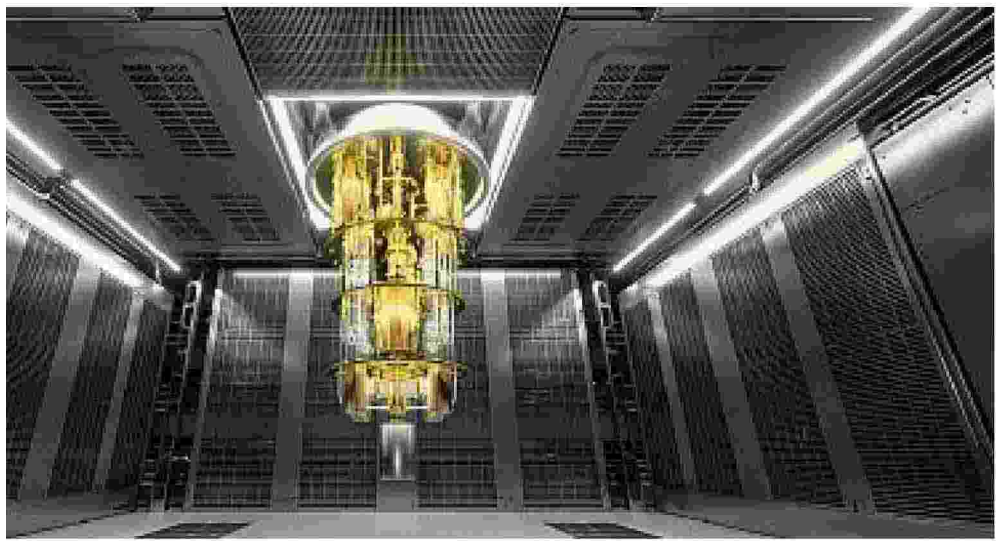
Fondazione Compagnia di San Paolo

CORRIERE TORINO L'Economia NORD OVEST

Il profilo

Andrea Vesco, 45 anni, torinese, si è laureato in ingegneria informatica e di sistema presso il Politecnico di Torino, nel 2009

Oggi è a capo della ricerca sulla cybersecurity di Fondazione Links, un centro di ricerca senza scopo di lucro



Computer quantistico
Se da una parte permetterà di ottenere importanti risultati in quasi tutti i settori, dall'altra rischia di rompere qualsiasi sistema di sicurezza informatico