UNIMORE
UNIVERSITÀ DEGLI STUDI DI MODENA E REGGIO EMILIA

Dipartimento di Ingegneria "Enzo Ferrari"

AVVISO DI SEMINARIO

21 novembre 2017, ora 14.15
Dipartimento di Ingegneria Enzo Ferrari
Edificio 25, Aula FA-1F

SICUREZZA E TECNOLOGIE QUANTISTICHE

Potenziali usi e rischi in ambito sicurezza

Enrico Prati, Consiglio Nazionale delle Ricerche

Cosa sono e come funzionano i computer quantistici? Quali applicazioni sono possibili in ambito sicurezza? L'algoritmo che ha ispirato il loro sviluppo nei primi anni 2000 è stato quello di Shor per la fattorizzazione in numeri primi che, in linea di principio, sono in grado di rendere inutilizzabili la maggior parte degli attuali sistemi di cifratura. Contemporaneamente, sono stati sviluppati nuovi metodi di comunicazione quantistica teoricamente sicura, a loro volta basati sulla meccanica quantistica. Tuttavia i computer quantistici, con la loro grande potenza di calcolo, possono fare molto di più che violare un codice di cifratura, e le stesse comunicazioni quantistiche non sono immuni da vulnerabilità connesse al tipo di implementazione.
Nel seminario, si introducono due recenti famiglie di tecnologie costituite dalle comunicazioni e dai computer quantistici, i loro rispettivi algoritmi, gli attori governativi e privati che hanno investito su di esse, e i rischi connessi al loro impiego.

Enrico Prati è ricercatore presso l'Istituto di Fotonica e Nanotecnologie del CNR di Milano ove si interessa di informazione quantistica. Dal 2014 è Visiting Scholar presso la Waseda University a Tokyo. È stato Keynote Speaker a IEDM 2014 a San Francisco, la principale conferenza di elettronica, speaker al TEDx di Roma nel 2016 con un contributo sull'intelligenza artificiale quantistica e a ICRC Rebooting Computing a Washington del 2017. Nel settembre 2017 ha pubblicato il libro "Mente Artificiale" con l'editore EGEA.