SOLUZIONI QUANTISTICO-CLASSICHE PER OTTIMIZZAZIONE E RILEVAMENTO DI ANOMALIE

Leonardo Lavagna, Andrea Ceschini, Simone Piperno, Marco Casalbore, Antonello Rosato, Massimo Panella

Dipartimento di Ingegneria dell'Informazione, Elettronica e Telecomunicazioni (DIET)
Università degli Studi di Roma "La Sapienza"
Via Eudossiana, 18, 00184 Roma

Il calcolo quantistico, nella sua fase attuale caratterizzata da dispositivi Noisy Intermediate-Scale Quantum (NISQ) [1], sta mostrando un potenziale crescente nella risoluzione di problemi di ottimizzazione combinatoria e apprendimento automatico, tipicamente difficili da scalare con approcci classici [2]. L'emergere di algoritmi variazionali, come il Quantum Approximate Optimization Algorithm (QAOA) e le Quantum Neural Networks (QNN), ha aperto la strada a nuove architetture ibride (v. Fig. 1) che uniscono la potenza espressiva del machine learning con l'efficienza esplorativa dei circuiti quantistici [3]. In questo contesto, l'utilizzo di rappresentazioni binarie (QUBO) e di matrici unitarie parametrizzate nello spazio di Hilbert che codifica i problemi da risolvere è un elemento chiave per costruire pipeline robuste con *hardware* quantistico [4].

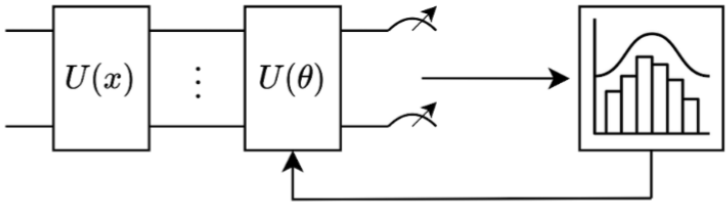

Figura 1 – Schema di QNN basata su un circuito variazionale dato da un blocco di matrici unitarie *U(x)* di codifica dei dati e un blocco di matrici unitarie parametrizzate *U(Θ)* e addestrabili.

All'interno di questo quadro si inseriscono tre filoni applicativi sinergici, volti a esplorare le connessioni tra ottimizzazione, apprendimento automatico e calcolo quantistico: la rilevazione di anomalie in serie temporali, l'ottimizzazione su strutture a grafo, e la crittografia in ambienti classico-quantistici. Nel primo ambito di ricerca, è stato sviluppato un framework ibrido per la rilevazione di anomalie in serie temporali, basato su una formulazione QUBO e risolto tramite QAOA [5]. Il modello consente di integrare metodi statistici in una funzione obiettivo quantistica, identificando anomalie anche in dati rumorosi o scarsamente etichettati, con applicazioni nei settori industriale, biomedicale ed energetico. Parallelamente, è stata studiata l'influenza delle simmetrie nei grafi sul comportamento del QAOA nella risoluzione di problemi MaxCut, prototipi di problemi NP-hard [6]. Ciò ha portato allo sviluppo di euristiche per la semplificazione dei circuiti e per il trasferimento di parametri ottimali da istanze semplici a più complesse, abilitando strategie di addestramento ricorsivo. In ambito crittografico, è stato analizzato il compromesso tra sicurezza ed efficienza nei crittosistemi, modellando l'interazione tra circuiti booleani e quantistici in schemi basati su funzioni botola. Attraverso una reinterpretazione quantistica delle costruzioni classiche, sono state studiate condizioni di sicurezza su dispositivi NISQ (v. Fig. 2), incluse varianti basate su camminate quantistiche e Grover [7]. I risultati ottenuti sono stati poi estesi a modelli variazionali, evidenziando nuovi scenari di resilienza e vulnerabilità computazionale.

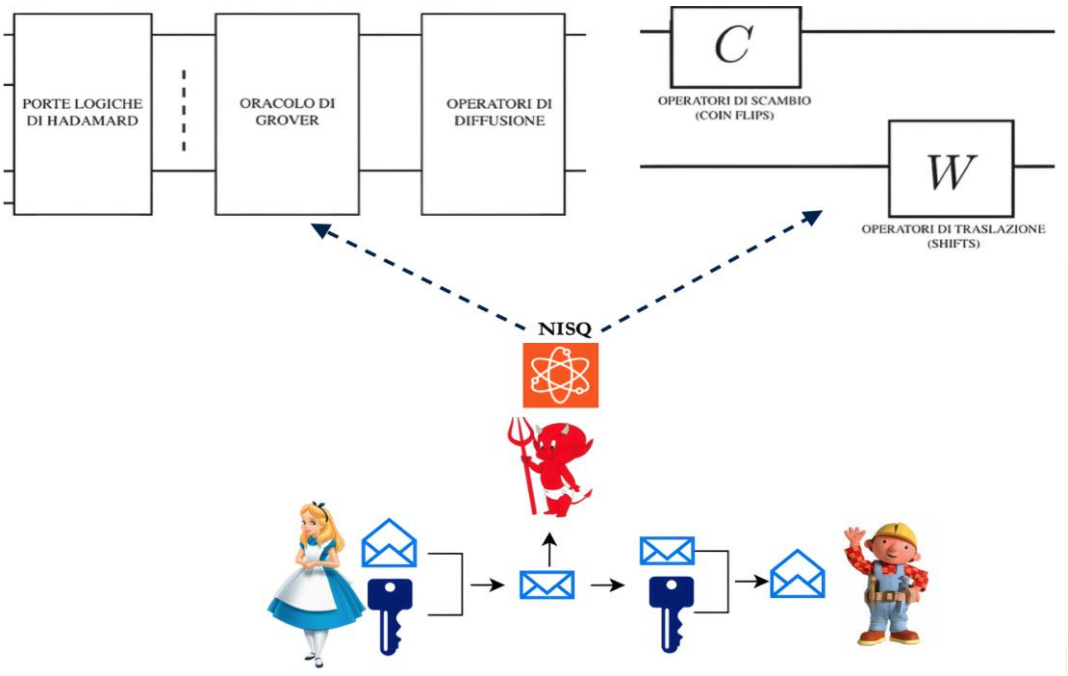

Figura 2 – Schema di un possibile attacco con dispositivi NISQ di un sistema di cifratura-decifratura simmetrico. Un attaccante con accesso a dispositivi quantistici attuali può utilizzare o un circuito variazionale o una passeggiata quantistica. In entrambi i casi l'attacco, essendo basato su dispositivi NISQ, può produrre risultati poco robusti, non comparabili coi più sofisticati attacchi classici.

Come studio complementare, è stato realizzato un tutorial dedicato alla teoria delle perturbazioni per l'equazione di Schrödinger unidimensionale [9]. Il lavoro, pensato per ingegneri e ricercatori, fornisce una trattazione chiara e applicativa dei metodi perturbativi diretti e indiretti, con esempi su potenziali quantistici classici e distribuzioni generalizzate come la delta di Dirac, oltre che per analizzare l'effetto di perturbazioni su strutture QUBO o su grafi, e guidare l'adattamento di circuiti variazionali in presenza di deviazioni controllate.

La presente ricerca è stata svolta nell'ambito del ***"CENTRO NAZIONALE PER HPC, BIG DATA E COMPUTAZIONE QUANTUM" (CN1, Spoke 10), PNRR - Missione 4 - Componente 2 - Investimento 1.4****, finanziato dall'Unione Europea – Next generation EU, CN00000013, CUP B83C22002940006.*

Riferimenti bibliografici

[1] J. Preskill, "Quantum Computing in the NISQ era and beyond", *Quantum*, p. 79. 2018.

[2] A. Montanaro, "Quantum algorithms: An overview", *npj Quantum Information*, 2015

[3] M. Panella, G. Martinelli. "Neural networks with quantum architecture and quantum learning", *International Journal of Circuit Theory and Applications*. 39: 61–77, 2011.

[4] M. Benedetti, E. Lloyd, S. Sack, M. Fiorentini, "Parameterized quantum circuits as machine learning models", *Quantum Science and Technology* 4.4 p. 043001, 2019.

[5] V. Chandola, A. Banerjee, V. Kumar, "Anomaly detection: A survey", *ACM computing surveys (CSUR)*, vol. 41, no. 3, pp. 1–58, 2009.

[6] L. Lavagna, S. Piperno, A. Ceschini, M. Panella, "On the effects of small graph perturbations in the maxcut problem by QAOA", *arXiv preprint*, arXiv:2408.15413, 2024.

[7] R. Gennaro, Y. Gertner, J. Katz, L. Trevisan, "Bounds on the efficiency of generic cryptographic constructions", *SIAM Journal on Computing*, vol. 35, no. 1, pp. 217–246, 2005.

[8] T. Kato, "Perturbation Theory for Linear Operators", *Springer Vol. 13 in the series: Grundlehren der mathematischen Wissenschaften*. 2nd ed., 1995.