

TITOLO: Tecniche di Valutazione delle Risorse per Programmi Quantistici

PROGETTO DI RICERCA

Il progetto prevede la simulazione di un attacco quantistico contro un cifrario a chiave pubblica quale RSA. Verranno analizzate e studiate metodologie innovative, in modo da comprenderne i limiti ma anche informando il design di nuovi attacchi. L'obiettivo è studiare in che misura i computer quantistici possono decrittare un messaggio protetto dalla crittografia RSA considerando i due approcci seguenti:

- Annealing quantistico;
- Algoritmi di fattorizzazione variazionale quantistica (VQF).

PIANO ATTIVITÀ

Il laureato reclutato nel progetto si occuperà di studiare lo stato nell'arte rispetto all'implementazione concreta di attacchi quantistici contro cifrari quali RSA, per poi progettare, implementare e valutare alcuni di tali approcci.